

# Secret-Key Generation Using Compound Sources and One-Way Public Communication

Nima Tavangaran, *Student Member, IEEE*, Holger Boche, *Fellow, IEEE*, and Rafael F. Schaefer, *Member, IEEE*

**Abstract**—In the classical Secret-Key generation model, Common Randomness is generated by two terminals based on the observation of correlated components of a common source, while keeping it secret from a non-legitimate observer. It is assumed that the statistics of the source are known to all participants. In this work, the Secret-Key generation based on a compound source is studied where the realization of the source statistic is unknown. The protocol should guarantee the security and reliability of the generated Secret-Key, simultaneously for all possible realizations of the compound source. A single-letter lower-bound of the Secret-Key capacity for a finite compound source is derived as a function of the public communication rate constraint. A multi-letter capacity formula is further computed for a finite compound source for the case in which the public communication is unconstrained. Finally a single-letter capacity formula is derived for a degraded compound source with an arbitrary set of source states and a finite set of marginal states.

**Index Terms**—Compound source, Secret-Key capacity, Common Randomness, hypothesis testing.

## I. INTRODUCTION

Current cryptographic approaches are dependent on the computational capabilities of the non-legitimate terminals. By increasing technological advances, the security of transmitted information can not be guaranteed for sure. In contrast, an information theoretic approach provides us with a framework for future coding schemes that guarantee security independent of computational capabilities of the eavesdroppers.

Information theoretic security was first introduced by Shannon in [1]. In the so called one-time pad method, each transmitting message is encrypted by a Secret-Key (SK). If there is no SK available, it has to be generated first. One approach is to generate a shared SK based on a common source. In this model, two terminals observe correlated components of a common source and communicate over a public noiseless channel to generate a common SK. Afterwards, they can encrypt subsequent communication using this SK. This procedure relies on the generation of Common Randomness (CR) which was introduced in [2] and later used by Maurer in [3] and Ahlswede and Csiszár in [4] to determine the SK capacity. The SK sharing

is further studied in [5]–[9]. In practice, this kind of security can be integrated in the physical layer of wireless systems [10].

However, in all these models which were used for SK generation, perfect knowledge of the source statistics was assumed. In a more general approach, the source uncertainty should be taken into account where the terminals do not have the knowledge of the actual realization of the source. An achievable SK rate for a compound Discrete Memoryless Multiple Source (DMMS)  $\{(X, Y_s, Z_s)\}_{s \in \mathcal{S}}$  was given in [11]. In [12], the compound DMMS  $\{(X_s, Y_s)\}_{s \in \mathcal{S}}$  was studied and the SK capacity was computed. As related problems, compound source coding, SK generation with Arbitrarily Varying Channel (AVC), compound wiretap channels and robust biometric authentication were studied in [13]–[18].

In this work, a SK generation model for a compound DMMS with one-way communication in presence of an eavesdropper is studied. The terminals observe a compound source  $\mathfrak{S} := \{XYZ, s\}_{s \in \mathcal{S}} := \{(X_s, Y_s, Z_s)\}_{s \in \mathcal{S}}$ , and two of them generate a shared SK by using only a one-way communication over a public noiseless channel while keeping it secret from the third terminal (eavesdropper). As the source realization index  $s \in \mathcal{S}$  is unknown to the terminals, an estimation method such as hypothesis testing is incorporated to find the marginal source index of the transmitter. This approach is used to generalize the result in [5, Theorem 2.6], [7, Theorem 17.21] to the compound setup for the source  $\mathfrak{S}$ .

In Section II, the model for SK generation is presented. Section III gives the main results. A single-letter lower-bound for the SK capacity of a finite compound source is derived as a function of the communication rate constraint over the public channel. A multi-letter SK capacity formula is computed as well for the case where the public communication rate is unconstrained. We proposed these two results which are stated in Theorems 1 and 2, originally in [19] in which the proof ideas have been outlined. In the present paper, in contrast, we give the complete proofs of both theorems as well as the proofs for random coding and security lemmas. The third and main result of this work which is not available in [19] gives a single-letter SK capacity formula for a degraded compound source, where the set of source states may be infinite and the set of marginal states is finite. Compared with previous theorems, this result which is stated in Theorem 3 is more practical in the sense that the SK capacity is single-letter and also valid for sources with an infinite set of source states  $\mathcal{S}$ . The complete formal proofs are given in Section IV. Section V concludes the paper.

**Notation:**  $\mathbb{R}$  and  $\mathbb{N}$  denote the set of real numbers and natural numbers respectively. The complement of a set  $\mathcal{A}$  is denoted by  $\mathcal{A}^c$  and the subtraction of two sets  $\mathcal{A}$  and  $\mathcal{B}$

This work was presented in part at IEEE-ITW, Jeju Island, Korea, 2015.

N. Tavangaran and H. Boche are with Lehrstuhl für Theoretische Informationstechnik, Technische Universität München, 80290 München, Germany, e-mail: nima.tavangaran@tum.de, boche@tum.de

R. F. Schaefer was with the Department of Electrical Engineering, Princeton University, NJ 08544, USA. He is now with Technische Universität Berlin, 10587 Berlin, Germany, email: rafael.schaefer@tu-berlin.de

This work of N. Tavangaran and H. Boche was supported by the German Research Foundation (DFG) under grant BO 1734/20-1.

This work of R. F. Schaefer was supported by the German Research Foundation (DFG) under grant WY 151/2-1.

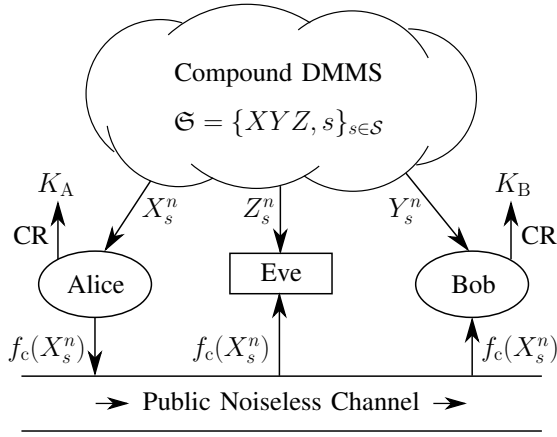


Fig. 1: SK generation protocol for compound DMMS model

is given by  $\mathcal{A} - \mathcal{B} := \mathcal{A} \cap \mathcal{B}^c$ . The underlying probability measure is represented by  $\Pr$ . The  $\log(\cdot)$  and  $\exp(\cdot)$  are to the basis 2 and  $\ln(\cdot)$  is the natural logarithm to the basis e. For any function  $f$ , the cardinal number of the range of the function is denoted by  $\|f\|$ . Random Variables (RVs) are denoted by capital letters (e.g.  $X^n, U, \dots$ ), their realizations by small letters (e.g.  $x^n, u, \dots$ ), their ranges (alphabets) by script letters (e.g.  $\mathcal{X}^n, \mathcal{U}, \dots$ ), and their Probability Distributions (PDs) by Roman letters (e.g.  $P_{X^n}, P_U, \dots$ ). All alphabets corresponding to RVs are supposed to be finite.  $H(X)$  and  $I(X; Y)$  represent the entropy of a RV  $X$  and the mutual information between  $X$  and  $Y$  respectively.  $h(a)$  with  $a \in [0, 1]$  is the binary entropy function and is given by  $h(a) := -a \log a - (1 - a) \log(1 - a)$ . For any two probability measures  $P$  and  $Q$ ,  $\|P - Q\| := \sum_{x \in \mathcal{X}} |P(x) - Q(x)|$  denotes their 1-norm distance.  $\mathbb{1}_{\mathcal{A}}(\cdot)$  denotes the indicator function for a set  $\mathcal{A}$ .  $\mathbb{E}_U[X]$  represents the expectation of a RV  $X$  with respect to the RV  $U$ . A stochastic matrix  $W : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{Y})$  is a function from the set  $\mathcal{X}$  to  $\mathcal{P}(\mathcal{Y})$ , where  $\mathcal{P}(\mathcal{Y})$  is the set of all PDs defined on the set  $\mathcal{Y}$ . Finally,  $X - Y - Z$  denotes a Markov chain for RVs  $X$ ,  $Y$ , and  $Z$ .

## II. SK GENERATION MODEL

Figure 1 shows the SK generation model which is used throughout this work. Transmitter (Alice), receiver (Bob) and eavesdropper (Eve) observe a compound DMMS  $\mathfrak{S} = \{XYZ, s\}_{s \in \mathcal{S}}$  for time duration  $n \in \mathbb{N}$ . It is assumed that all terminals know the set of source states  $\mathcal{S}$  as well as its statistics with PDs  $\{P_{XYZ, s}\}_{s \in \mathcal{S}}$ . However, they do not have the knowledge of the actual realization  $s \in \mathcal{S}$  of the source statistic. Therefore, RVs  $X_s^n, Y_s^n$  and  $Z_s^n$  represent their initial knowledge for the source state  $s \in \mathcal{S}$ . The next definition describes the model which is studied through out this work.

**Definition 1.** The SK generation model consists of a transmitter (Alice), a receiver (Bob), an eavesdropper (Eve), a compound DMMS by which their initial knowledge is given, and a public noiseless communication channel between all terminals. The source is given for an arbitrary set of states  $\mathcal{S}$ , by a sequence of generic RVs  $\mathfrak{S} = \{XYZ, s\}_{s \in \mathcal{S}}$  taking their values in the finite set  $\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ .

As RVs  $X_s^n$  and  $Y_s^n$  are correlated, Alice and Bob may generate some CR by communicating over the public channel. In this work, only a one-way communication over the public channel, initiated by Alice, is allowed. The following definition gives a more precise description of this procedure.

**Definition 2.** A one-way SK generation protocol for the model in Definition 1 with source  $\mathfrak{S} = \{XYZ, s\}_{s \in \mathcal{S}}$  consists of the following two steps:

- After observing  $X_s^n$ , Alice transmits a message  $f_c(X_s^n)$  to Bob over the public noiseless channel.  $f_c$  is called public communication function.<sup>1</sup>
- Next, Alice generates a SK, represented by a RV  $K_A$ , based on her knowledge  $X_s^n$  and Bob generates a SK, represented by a RV  $K_B$ , based on his knowledge  $(Y_s^n, f_c(X_s^n))$ .  $K_A$  and  $K_B$  take their values in  $\mathcal{K}$ .

As the communication over the public channel is overheard by Eve, this should not reveal any information about the SK. Moreover, the generated SK should have a uniform distribution. Combining these two criteria together leads to a compact notion, called security index, which was first introduced in [6].

**Definition 3.** For RVs  $K_A$  and  $V$ , taking values in the sets  $\mathcal{K}$  and  $\mathcal{V}$  respectively, the security index is given by

$$S(K_A|V) := \log(|\mathcal{K}|) - H(K_A) + I(K_A; V).$$

In our context,  $K_A$  represents the SK and  $V$  Eve's knowledge. This short notion is a powerful tool which can be used to describe both strong secrecy [20] and the uniformity of the generated SK. The next definition, uses this concept to define an achievable SK rate and capacity of a compound source.

**Definition 4.** A real number  $R_{\text{sk}} \geq 0$  is an achievable SK rate for the model in Definition 1 with compound source  $\mathfrak{S} = \{XYZ, s\}_{s \in \mathcal{S}}$  and a one-way communication over the public noiseless channel with rate constraint  $\Gamma \in (0, +\infty]$ , if and only if, for all  $\delta > 0$ , and all  $n \in \mathbb{N}$  large enough, there exists a SK generation protocol with public communication function  $f_c$ , giving rise to the RVs  $K_A$  and  $K_B$  with values in  $\mathcal{K}$ , for which it holds:

$$\frac{1}{n} \log \|f_c\| < \Gamma + \delta, \quad (1)$$

$$R_{\text{sk}} < \frac{1}{n} \log |\mathcal{K}| + \delta, \quad (2)$$

$$\forall s \in \mathcal{S}, \quad \Pr(K_A \neq K_B) < \delta, \quad (3)$$

$$\forall s \in \mathcal{S}, \quad S(K_A|Z_s^n, f_c(X_s^n)) < \delta. \quad (4)$$

The SK capacity  $C_{\text{sk}}(\mathfrak{S}, \Gamma)$  for this model is defined to be the supremum of all achievable SK rates. If there is no communication rate constraint, i.e.  $\Gamma = \infty$ , then condition (1) in the definition is inactive and the capacity is simply denoted by  $C_{\text{sk}}(\mathfrak{S})$ .

Similarly as in [5], [7], the communication rate constraint is also part of the achievability definition. This is because, in a

<sup>1</sup>Similarly as in [7, Problem 17.15(a)], it can be shown that a randomized  $f_c$  in the one-way SK generation protocol does not increase the SK capacity. Therefore, the communication function  $f_c$  is assumed to be a deterministic function of  $X_s^n$  and no randomization is considered here.

realistic model where the communication cost is an important parameter, the information exchange rate between the terminals is restricted.

In the following, a subset of the compound set  $\mathcal{S}$  is defined. This definition is required for stating the results in Section III.

**Definition 5.** Let for the compound source  $\mathfrak{S} = \{XYZ, s\}_{s \in \mathcal{S}}$ ,  $\hat{\mathcal{S}}$  be the set of all possible states of marginal RV  $X$ . For a given marginal state  $\hat{s} \in \hat{\mathcal{S}}$ , corresponding to the RV  $X_{\hat{s}}$ , the set of all possible source states is given by

$$\mathcal{I}(\hat{s}) := \left\{ s \in \mathcal{S} : \forall x \in \mathcal{X}, \sum_{y \in \mathcal{Y}} \sum_{z \in \mathcal{Z}} P_{XYZ,s}(x, y, z) = P_{X_{\hat{s}}}(x) \right\}. \quad (5)$$

### III. SK CAPACITY RESULTS

In this section, SK capacity results of compound DMMS models are presented. Moreover, short proof sketches are provided for the first and third theorems. The complete formal proofs are given in Section IV. For all theorems which are stated in this section, the sets  $\hat{\mathcal{S}}$  and  $\mathcal{I}(\hat{s})$  are given by Definition 5.

In the following, Theorem 1 gives a single-letter lower-bound for the capacity of a compound DMMS source model with a finite set of source states where the public communication rate is limited.

**Theorem 1.** For a finite compound DMMS model with a source  $\mathfrak{S} = \{XYZ, s\}_{s \in \mathcal{S}}$  and a one-way communication over a public noiseless channel with constraint  $\Gamma \in (0, \infty]$ , it holds:

$$C_{\text{sk}}(\mathfrak{S}, \Gamma) \geq \min_{\hat{s} \in \hat{\mathcal{S}}} \max_{U_{\hat{s}}, V_{\hat{s}}} \left\{ \min_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Y_s | U_{\hat{s}}) - \max_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Z_s | U_{\hat{s}}) \right\}, \quad (6)$$

where the outer max is taken over all RVs  $U_{\hat{s}}$  and  $V_{\hat{s}}$  such that it holds:

$$\forall s \in \mathcal{I}(\hat{s}), U_{\hat{s}} - V_{\hat{s}} - X_{\hat{s}} - Y_s Z_s \quad \text{and} \quad \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; X_{\hat{s}} | Y_s) + \max_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; X_{\hat{s}} | U_{\hat{s}} Y_s) < \Gamma. \quad (7)$$

*Proof sketch:* To achieve the SK rate in (6), Alice estimates her marginal state  $\hat{s} \in \hat{\mathcal{S}}$  by hypothesis testing such that the estimation error is exponentially small [21]. Similarly as in [12], she sends this along with other information related to her observation over the public channel to Bob. In Figure 1, this is denoted by  $f_c(X_{\hat{s}}^n)$ . Given an estimated marginal source state of Alice  $\hat{s} \in \hat{\mathcal{S}}$ , the joint source state  $s$  is not necessarily known to the terminals. However, by Definition 5, it is known that  $s \in \mathcal{I}(\hat{s})$ .

For the correctly estimated Alice's state, say  $\hat{s} \in \hat{\mathcal{S}}$ , Lemma 7 from Subsection IV-A, assures that Alice and Bob can generate some CR by using their knowledge with an exponentially small error. This CR is universal for all source states  $s \in \mathcal{I}(\hat{s})$ .

Furthermore, the public communication rate should be lower than a given  $\Gamma > 0$ . Therefore, the coding scheme, introduced in Lemma 7, should work with respect to this limitation which is given by (7). This problem for the case where no communication constraint is given is easier to solve and a non-compound version is available in [7, Problem 17.15b].

Finally, as seen in Figure 1, Alice and Bob generate their SKs  $K_A$  and  $K_B$  based on the CR by using a SK generator. However,  $f_c(X_{\hat{s}}^n)$  is also received by Eve. Lemma 8, again from Subsection IV-A, assures the existence of a SK generator which guarantees the strong secrecy and the uniformity of the SK  $K_A$ , for all possible  $s \in \mathcal{I}(\hat{s})$ .  $\square$

As a second result, a multi-letter SK capacity formula is computed for the case, in which no communication rate constraint is given and the set of source states is again finite.

**Theorem 2.** For a finite compound DMMS model with a source  $\mathfrak{S} = \{XYZ, s\}_{s \in \mathcal{S}}$  and a one-way communication over a public noiseless channel, it holds:

$$C_{\text{sk}}(\mathfrak{S}) = \lim_{n \rightarrow \infty} \frac{1}{n} \min_{\hat{s} \in \hat{\mathcal{S}}} \max_{U_{\hat{s}}, V_{\hat{s}}} \left\{ \min_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Y_s^n | U_{\hat{s}}) - \max_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Z_s^n | U_{\hat{s}}) \right\}, \quad (8)$$

where the outer max is taken over all RVs  $U_{\hat{s}}$  and  $V_{\hat{s}}$  such that it holds:

$$\forall s \in \mathcal{I}(\hat{s}), U_{\hat{s}} - V_{\hat{s}} - X_{\hat{s}}^n - Y_s^n Z_s^n. \quad (9)$$

Finally as the main result, a single-letter SK capacity formula is given in the following for a degraded compound source with an arbitrary set of source states  $\mathcal{S}$  which might be infinite.

**Theorem 3.** Consider a compound DMMS model with a source  $\mathfrak{S} = \{XYZ, s\}_{s \in \mathcal{S}}$  with an arbitrary set  $\mathcal{S}$ , a finite set of marginal states  $\hat{\mathcal{S}}$ , and a one-way communication over a public noiseless channel. If the following Markov chains are satisfied,

$$\forall \hat{s} \in \hat{\mathcal{S}}, \forall r, t \in \mathcal{I}(\hat{s}), X_{\hat{s}} - Y_r - Z_t, \quad (10)$$

then it holds:

$$C_{\text{sk}}(\mathfrak{S}) = \min_{\hat{s} \in \hat{\mathcal{S}}} \left\{ \inf_{r \in \mathcal{I}(\hat{s})} I(X_{\hat{s}}; Y_r) - \sup_{t \in \mathcal{I}(\hat{s})} I(X_{\hat{s}}; Z_t) \right\}. \quad (11)$$

*Proof sketch:* In the first step, the achievability result from Theorem 1 is used to show that the SK rate in (11) is achievable for a finite set of source states  $\mathcal{S}$ .

Next, for the infinite source  $\mathfrak{S} = \{XYZ, s\}_{s \in \mathcal{S}}$ , fix the marginal PD  $P_{X_{\hat{s}}}$  and define the infinite family of stochastic matrices  $\{P_{Y Z, s | X_{\hat{s}}} : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{Y} \times \mathcal{Z})\}_{s \in \mathcal{I}(\hat{s})}$ . By using Lemma 5 from Subsection IV-A, it follows that there exists a finite family of stochastic matrices  $\{W_{s'} : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{Y} \times \mathcal{Z})\}_{s' \in \mathcal{I}'(\hat{s})}$ , which approximates the infinite family. The finite set  $\mathcal{I}'(\hat{s})$  contains all indices of this finite family for the given  $\hat{s}$ .

Define the finite source  $\mathfrak{S}' := \{XYZ, s'\}_{s' \in \mathcal{I}'(\hat{s}), \hat{s} \in \hat{\mathcal{S}}}$  by  $P_{XYZ, s'}(x, y, z) := P_{X_{\hat{s}}}(x) W_{s'}(y, z | x)$  for all  $s' \in \mathcal{I}'(\hat{s})$ ,  $\hat{s} \in \hat{\mathcal{S}}$ , and  $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ . It is shown that the SK generation protocol, which is used for the finite source  $\mathfrak{S}'$ , also guarantees the achievability of the given rate in (11) for the infinite source  $\mathfrak{S}$ .  $\square$

The orders of Markov chains in Theorem 3 are crucial in determining the SK capacity. For example, assume that the orders of (10) are changed as given in the following,

$$\forall \hat{s} \in \hat{\mathcal{S}}, \forall r, t \in \mathcal{I}(\hat{s}), X_{\hat{s}} - Z_t - Y_r.$$

In this case the capacity is  $C_{\text{sk}}(\mathfrak{S}) = 0$ . This is because, by [4, Theorem 1], it holds that

$$\forall \hat{s} \in \hat{\mathcal{S}}, \forall r, t \in \mathcal{I}(\hat{s}), C_{\text{sk}}(\mathfrak{S}) \leq I(X_{\hat{s}}; Y_r | Z_t) = 0.$$

#### IV. PROOFS

This section is divided into 3 parts. Subsection IV-A gives a short review of definitions and results which are required in the proofs. In Subsection IV-B, Lemmas 7 and 8 for random coding and security are presented. Finally, Subsection IV-C presents the formal proofs of Theorems 1, 2, and 3.

##### A. Preliminaries

For the typical sequences and their related sets the same definitions as in [7, Chapters 2 and 17] are taken. Let  $N(x|x^n)$  give the number of repetitions of an element  $x$  in the sequence  $x^n$  and  $N(x, y|x^n, y^n)$  the number of repetitions of the pair  $(x, y)$  in the pair sequence  $(x^n, y^n)$ . For two RVs  $X$  and  $Y$  and stochastic matrix  $P_{Y|X} : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{Y})$ , the following definitions are used when  $\epsilon > 0$ :

$$\begin{aligned} \mathcal{T}_{[XY]\epsilon}^n &:= \left\{ (x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : \forall (x, y) \in \mathcal{X} \times \mathcal{Y}, \right. \\ &\quad \left| P_{XY}(x, y) - \frac{1}{n} N(x, y|x^n, y^n) \right| \leq \epsilon \\ &\quad \wedge (P_{XY}(x, y) = 0 \Rightarrow N(x, y|x^n, y^n) = 0) \left. \right\}, \\ \mathcal{T}_{[Y|X]\epsilon}^n(x^n) &:= \left\{ y^n \in \mathcal{Y}^n : \forall (x, y) \in \mathcal{X} \times \mathcal{Y}, \right. \\ &\quad \left| \frac{1}{n} N(x|x^n) P_{Y|X}(y|x) - \frac{1}{n} N(x, y|x^n, y^n) \right| \leq \epsilon \\ &\quad \wedge (P_{Y|X}(y|x) = 0 \Rightarrow N(x, y|x^n, y^n) = 0) \left. \right\}, \\ \mathcal{T}_{[XY]\epsilon}(x^n) &:= \left\{ y^n \in \mathcal{Y}^n : (x^n, y^n) \in \mathcal{T}_{[XY]\epsilon}^n \right\}. \end{aligned}$$

In the following, a series of lemmas and propositions is provided which will be used in the proofs.

**Lemma 1** ([7]). *Let  $U, X$ , and  $Y$  be RVs taking value in  $\mathcal{U}, \mathcal{X}$ , and  $\mathcal{Y}$  respectively. Assume  $0 < \xi < \zeta < \sigma$ , and  $\tau > 0$  are all in  $\mathbb{R}$  and  $n \in \mathbb{N}$ . Then, it holds that*

- 1)  $\forall x^n \in \mathcal{T}_{[X]\xi}^n, \mathcal{T}_{[XY]\zeta}^n(x^n) \supset \mathcal{T}_{[Y|X]\zeta-\xi}^n(x^n)$ .
- 2)  $P_X^n(\mathcal{T}_{[X]\xi}^n) \geq 1 - 2|\mathcal{X}|e^{-2\xi^2 n}$ .
- 3)  $\forall \tau > 0, \forall \xi > 0$  sufficiently small, and  $\forall x^n \in \mathcal{T}_{[X]\xi}^n$ , it holds  $\left| -\frac{1}{n} \log P_X^n(x^n) - H(X) \right| < \tau$ .
- 4)  $\forall \tau > 0, \forall \xi > 0$  sufficiently small, and  $\forall n \in \mathbb{N}$  sufficiently large, it holds  $\left| \frac{1}{n} \log |\mathcal{T}_{[X]\xi}^n| - H(X) \right| < \tau$ .
- 5)  $\forall \tau > 0, \forall \zeta > 0$  sufficiently small,  $\forall n \in \mathbb{N}$  sufficiently large, and  $\forall u^n$  with  $\mathcal{T}_{[UX]\zeta}^n(u^n) \neq \emptyset$  it holds  $\left| \frac{1}{n} \log |\mathcal{T}_{[UX]\zeta}^n(u^n)| - H(X|U) \right| < \tau$ .
- 6) For  $U - X - Y$  and  $\forall (u^n, x^n) \in \mathcal{T}_{[UX]\xi}^n$  it holds  $P_{Y|X}^n(\mathcal{T}_{[UXY]\sigma}^n(u^n, x^n)|x^n) \geq 1 - 2|\mathcal{U}||\mathcal{X}||\mathcal{Y}|e^{-2(\sigma-\xi)^2 n}$ .
- 7)  $\forall \tau > 0, \forall \zeta > 0$  sufficiently small,  $\forall n \in \mathbb{N}$  sufficiently large, and  $\forall y^n \in \mathcal{Y}^n$  if  $\mathcal{T}_{[XY]\zeta}^n(y^n) \neq \emptyset$  then it holds  $\left| -\frac{1}{n} \log P_X^n(\mathcal{T}_{[XY]\zeta}^n(y^n)) - I(X; Y) \right| < \tau$ .
- 8)  $\forall \tau > 0, \forall \zeta > 0$  sufficiently small,  $\forall n \in \mathbb{N}$  sufficiently large, and  $\forall (u^n, y^n) \in \mathcal{U}^n \times \mathcal{Y}^n$  if  $\mathcal{T}_{[UXY]\zeta}^n(u^n, y^n) \neq \emptyset$  then it holds  $\left| -\frac{1}{n} \log P_{X|U}^n(\mathcal{T}_{[UXY]\zeta}^n(u^n, y^n)|u^n) - I(X; Y|U) \right| < \tau$ .

**Lemma 2** ([7]). *Let RVs  $U$  and  $X$  take their values in  $\mathcal{U}$  and  $\mathcal{X}$  respectively. Consider  $N = \exp(nR)$  sequences  $u_l^n$  with  $l \in \mathcal{L} := \{1, 2, \dots, N\}$ , which are independently drawn by a PD  $P_U^n$  with  $I(U; X) < R$ . Then for all  $\tau \in (0, R - I(U; X))$ , all  $\zeta > 0$  sufficiently small, all  $n \in \mathbb{N}$  sufficiently large, and all  $x^n$  such that  $\mathcal{T}_{[UX]\zeta}^n(x^n) \neq \emptyset$ , it holds that*

$$\left| \frac{1}{n} \log \left| \{l \in \mathcal{L} : u_l^n \in \mathcal{T}_{[UX]\zeta}^n(x^n)\} \right| - (R - I(U; X)) \right| < \tau,$$

with a probability approaching one, doubly exponentially fast.

**Lemma 3** ([7]). *Let RVs  $U, V$ , and  $X$  take their values in  $\mathcal{U}, \mathcal{V}$ , and  $\mathcal{X}$  respectively. Consider  $N = \exp(nR)$  sequences  $v_l^n$  with  $l \in \mathcal{L} := \{1, 2, \dots, N\}$ , which are independently drawn by a PD  $P_{V|U}^n(\cdot|u^n)$  for a given  $u^n$  with  $I(V; X|U) < R$ . Then for all  $\tau \in (0, R - I(V; X|U))$ , all  $\sigma > 0$  sufficiently small, all  $n \in \mathbb{N}$  sufficiently large, and all  $x^n$  such that  $\mathcal{T}_{[UVX]\sigma}^n(u^n, x^n) \neq \emptyset$ , it holds that*

$$\left| \frac{1}{n} \log \left| \{l \in \mathcal{L} : v_l^n \in \mathcal{T}_{[UVX]\sigma}^n(u^n, x^n)\} \right| - (R - I(V; X|U)) \right| < \tau,$$

with a probability approaching one, doubly exponentially fast. This holds uniformly for all given  $u^n \in \mathcal{U}^n$ .

**Lemma 4** ([7], [22]). *Let  $\epsilon, \eta > 0$  and  $\lambda > 0$  all in  $\mathbb{R}$  and  $k \in \mathbb{N}$  be given and  $U$  be a RV taking value in  $\mathcal{U}$ . If  $P_U(\{u \in \mathcal{U} : P_U(u) \leq \frac{1}{\lambda}\}) \geq 1 - \eta$ , then for a randomly selected function  $\kappa : \mathcal{U} \rightarrow \{1, 2, \dots, k\}$  it holds,*

$$\Pr\left(\|\kappa(P_U) - P_0\| > \epsilon + 2\eta\right) \leq 2ke^{-\frac{\lambda\epsilon^2(1-\eta)}{2k(1+\epsilon)}},$$

where  $P_0(i) = 1/k$  for all  $i = 1, 2, \dots, k$ . Random selection means that the  $\kappa(u), u \in \mathcal{U}$  are chosen independently and identically distributed (iid) uniformly.

**Lemma 5** ([23]). *Let  $\mathcal{S}$  be an arbitrary set and possibly infinite and  $\{W_s : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{U})\}_{s \in \mathcal{S}}$  be a family of stochastic matrices. For every  $l \in \mathbb{N}$  with  $l \geq 2|\mathcal{U}|^2$ , there exists a family of stochastic matrices  $\{W_{s'} : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{U})\}_{s' \in \mathcal{S}'}$  with a finite set  $\mathcal{S}'$ , such that  $|\mathcal{S}'| \leq (l+1)^{|\mathcal{X} \times \mathcal{U}|}$ , where the following properties hold:  $\forall s \in \mathcal{S}, \exists s' \in \mathcal{S}', \forall x \in \mathcal{X}, \forall u \in \mathcal{U}$ ,*

$$|W_s(u|x) - W_{s'}(u|x)| \leq \frac{1}{l}|\mathcal{U}|, \quad W_s(u|x) \leq e^{2|\mathcal{U}|^2/l} W_{s'}(u|x).$$

**Lemma 6** ([24]). *Let  $(X, Y)$  and  $(X', Y')$  be two pairs of RVs taking values in  $\mathcal{X} \times \mathcal{Y}$  with PDs  $P_{XY}$  and  $P_{X'Y'}$  respectively. Furthermore, let  $\gamma := \frac{1}{2}\|P_{XY} - P_{X'Y'}\|$  and  $\gamma \leq 1 - \frac{1}{|\mathcal{X} \times \mathcal{Y}|}$ . Then, it holds that*

$$|I(X; Y) - I(X'; Y')| \leq 3\gamma \log(|\mathcal{X} \times \mathcal{Y}| - 1) + 3h(\gamma).$$

##### B. Random Coding and Security Lemmas

In this subsection, Lemmas 7 and 8 for finite compound sets with their proofs are presented. Similar techniques which are used in the non-compound versions in [7, Lemmas 17.5 and 17.22], [5], [25], are used in the following proofs and extended to the compound setup. For completeness, we present all proofs in detail. These lemmas are required for the proof of Theorem 1. Assume in Lemma 7, if the values in the equations (12), (13), (14), and (15) are not integer numbers, then the smallest integer which is larger than the given expression is taken.

**Lemma 7.** Let  $\delta > 0$  and  $\sigma > \zeta > 0$  be all in  $\mathbb{R}$  and sufficiently small. Furthermore, let Alice's state  $\hat{s} \in \hat{\mathcal{S}}$  be given and for all  $s \in \mathcal{I}(\hat{s})$ , RVs  $X_{\hat{s}}$  and  $Y_s$  take their values in  $\mathcal{X}$  and  $\mathcal{Y}$  respectively. Let also RVs  $U_{\hat{s}}$  and  $V_{\hat{s}}$  be given such that for all  $s \in \mathcal{I}(\hat{s})$  the Markov chains  $U_{\hat{s}} - V_{\hat{s}} - X_{\hat{s}} - Y_s$  hold.

Assume  $N_{\hat{s},1}N_{\hat{s},2}$  random sequences  $u_{ij}^n(\hat{s}) \in \mathcal{U}^n$ , chosen independently according to PD  $P_{U_{\hat{s}}}^n$ , are given and known to Alice and Bob where

$$i \in \mathcal{I} := \{1, 2, \dots, N_{\hat{s},1}\}, \quad j \in \mathcal{J} := \{1, 2, \dots, N_{\hat{s},2}\},$$

$$N_{\hat{s},1} := \exp \left[ n \left( \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; X_{\hat{s}} | Y_s) + 3\delta \right) \right], \quad (12)$$

$$N_{\hat{s},2} := \exp \left[ n \left( \min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) - 2\delta \right) \right]. \quad (13)$$

Moreover, let for each  $u_{ij}^n(\hat{s})$ ,  $N_{\hat{s},3}N_{\hat{s},4}$  random sequences  $v_{pq}^{ij,n}(\hat{s}) \in \mathcal{V}^n$ , chosen conditionally independently according to  $P_{V_{\hat{s}}|U_{\hat{s}}}^n(\cdot | u_{ij}^n(\hat{s}))$ , be given and known to Alice and Bob where

$$p \in \mathcal{P} := \{1, 2, \dots, N_{\hat{s},3}\}, \quad q \in \mathcal{Q} := \{1, 2, \dots, N_{\hat{s},4}\},$$

$$N_{\hat{s},3} := \exp \left[ n \left( \max_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; X_{\hat{s}} | U_{\hat{s}} Y_s) + 3\delta \right) \right], \quad (14)$$

$$N_{\hat{s},4} := \exp \left[ n \left( \min_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Y_s | U_{\hat{s}}) - 2\delta \right) \right]. \quad (15)$$

Then CR can be generated between Alice and Bob in two ways:

a) For  $n \in \mathbb{N}$  sufficiently large, there exist encoder functions  $f: \mathcal{T} \rightarrow \mathcal{I}$  and  $g: \mathcal{T} \rightarrow \mathcal{J}$ , with a probability approaching 1, doubly exponentially fast where

$$\mathcal{T} := \{x^n \in \mathcal{X}^n : \mathcal{T}_{[UX, \hat{s}]\zeta}^n(x^n) \neq \emptyset\}, \quad (16)$$

and if  $f(x^n) = i$ ,  $g(x^n) = j$  then  $(u_{ij}^n(\hat{s}), x^n) \in \mathcal{T}_{[UX, \hat{s}]\zeta}^n$ . Alice encodes her observation  $x^n \in \mathcal{T}$  by these functions to the sequence  $u_{ij}^n(\hat{s})$  where  $j$  is the CR.

For functions  $f$  and  $g$ , extending their domain to  $\mathcal{X}^n$  by defining for all  $x^n \notin \mathcal{T}$ ,  $f(x^n) = g(x^n) = 0$ , there exists a decoder  $\tilde{g}: \mathcal{I} \times \hat{\mathcal{S}} \times \mathcal{Y}^n \rightarrow \mathcal{J}$  such that for all  $s \in \mathcal{I}(\hat{s})$ ,

$$\Pr\{g(X_{\hat{s}}^n) \neq \tilde{g}(f(X_{\hat{s}}^n), \hat{s}, Y_s^n)\} < \exp(-n\delta_0), \quad (17)$$

for some  $\delta_0 > 0$ . Thus, Bob can reconstruct  $g(x^n) = j$  from  $(f(x^n), \hat{s}, y^n)$  for given realizations  $X_{\hat{s}}^n = x^n$  and  $Y_s^n = y^n$ .

b) For each  $f$  and  $g$  from part a), and  $n \in \mathbb{N}$  sufficiently large, there exist encoder functions  $\varphi: \mathcal{T} \rightarrow \mathcal{P}$  and  $\rho: \mathcal{T} \rightarrow \mathcal{Q}$  with a probability approaching 1, doubly exponentially fast, such that if  $f(x^n) = i$ ,  $g(x^n) = j$ ,  $\varphi(x^n) = p$ ,  $\rho(x^n) = q$  then  $(u_{ij}^n(\hat{s}), v_{pq}^{ij,n}(\hat{s}), x^n) \in \mathcal{T}_{[UVX, \hat{s}]\sigma}^n$ . Alice encodes her observation  $x^n \in \mathcal{T}$  by these functions to the sequence  $v_{pq}^{ij,n}(\hat{s})$  where  $q$  is the CR.

For functions  $\varphi$  and  $\rho$ , extending their domain to  $\mathcal{X}^n$  by defining for all  $x^n \notin \mathcal{T}$ ,  $\varphi(x^n) = \rho(x^n) = 0$ , there exists a decoder  $\tilde{\rho}: \mathcal{I} \times \mathcal{J} \times \mathcal{P} \times \hat{\mathcal{S}} \times \mathcal{Y}^n \rightarrow \mathcal{Q}$  such that for all  $s \in \mathcal{I}(\hat{s})$ ,

$$\Pr\{\rho(X_{\hat{s}}^n) \neq \tilde{\rho}(f(X_{\hat{s}}^n), g(X_{\hat{s}}^n), \varphi(X_{\hat{s}}^n), \hat{s}, Y_s^n)\} < \exp(-n\delta'_0), \quad (18)$$

for some  $\delta'_0 > 0$ . Thus, Bob can reconstruct  $\rho(x^n) = q$  from  $(f(x^n), g(x^n), \varphi(x^n), \hat{s}, y^n)$  for given realizations  $X_{\hat{s}}^n = x^n$  and  $Y_s^n = y^n$ .

*Proof:* a) Let  $R$  be the rate of choosing the sequences  $\{u_{ij}^n(\hat{s})\}_{(i,j) \in \mathcal{I} \times \mathcal{J}}$  which implies that  $N_{\hat{s},1}N_{\hat{s},2} = \exp(nR)$ . Therefore, by (12) and (13) and properties of the Markov chain, it follows that

$$\begin{aligned} R &= \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; X_{\hat{s}} | Y_s) + \min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) + \delta \\ &= I(U_{\hat{s}}; X_{\hat{s}}) + \max_{s \in \mathcal{I}(\hat{s})} [I(U_{\hat{s}}; Y_s | X_{\hat{s}}) - I(U_{\hat{s}}; Y_s)] \\ &\quad + \min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) + \delta = I(U_{\hat{s}}; X_{\hat{s}}) + \delta. \end{aligned} \quad (19)$$

Similarly as in [7, Lemma 17.22], for all  $x^n \in \mathcal{T}$ , it holds by the definition in (16) that  $\mathcal{T}_{[UX, \hat{s}]\zeta}^n(x^n) \neq \emptyset$ . Thus, Lemma 2 together with (19) implies for all  $\tau \in (0, R - I(U_{\hat{s}}; X_{\hat{s}}))$ , all  $\zeta > 0$  sufficiently small, all  $n \in \mathbb{N}$  sufficiently large, and all  $x^n \in \mathcal{T}$  that

$$\begin{aligned} \frac{1}{n} \log \left| \left\{ (i, j) \in \mathcal{I} \times \mathcal{J} : u_{ij}^n(\hat{s}) \in \mathcal{T}_{[UX, \hat{s}]\zeta}^n(x^n) \right\} \right| \\ \geq R - I(U_{\hat{s}}; X_{\hat{s}}) - \tau, \end{aligned}$$

with a probability approaching one, doubly exponentially fast. Therefore, for each  $x^n \in \mathcal{T}$ , the number of chosen sequences  $u_{ij}^n(\hat{s})$  which are in  $\mathcal{T}_{[UX, \hat{s}]\zeta}^n(x^n)$  is non-zero and the functions  $f$  and  $g$  as mentioned in the lemma, do exist with this probability.

Define for all  $i \in \mathcal{I}$  and  $y^n \in \mathcal{Y}^n$ , the decoder as follows:

$$\tilde{g}(i, \hat{s}, y^n) := \begin{cases} j & \text{if } j \in \mathcal{J}, u_{ij}^n(\hat{s}) \in \bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UY, s]\sigma|\mathcal{X}|}^n(y^n) \\ & \text{and } \forall m \in \mathcal{J}, m \neq j \Rightarrow \\ & \quad u_{im}^n(\hat{s}) \notin \bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UY, s]\sigma|\mathcal{X}|}^n(y^n) \\ 0 & \text{otherwise.} \end{cases} \quad (20)$$

Moreover, define

$$\begin{aligned} \mathcal{T}_0 &:= \{(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : x^n \in \mathcal{T} \\ &\quad \wedge (u_{f(x^n)g(x^n)}^n(\hat{s}), x^n, y^n) \in \bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UXY, s]\sigma}^n\}. \end{aligned}$$

In the following, it is shown that Alice and Bob's observation  $(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n$  is in the set  $\mathcal{T}_0$  with a probability exponentially close to one. It holds that

$$\begin{aligned} P_{XY, s}^n(\mathcal{T}_0^c) &= \sum_{x^n \in \mathcal{T}^c, y^n \in \mathcal{Y}^n} P_{XY, s}^n(x^n, y^n) + \sum_{x^n \in \mathcal{T}, (x^n, y^n) \notin \mathcal{T}_0} P_{XY, s}^n(x^n, y^n) \\ &= P_{X_s}^n(\mathcal{T}^c) + \sum_{x^n \in \mathcal{T}, (x^n, y^n) \notin \mathcal{T}_0} P_{X_s}^n(x^n) \\ &\quad \times P_{Y_s|X_s}^n \left( \bigcap_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UXY, s]\sigma}^c(u_{f(x^n)g(x^n)}^n(\hat{s}), x^n) | x^n \right). \end{aligned} \quad (21)$$

Lemma 1.1 implies for every  $x^n \in \mathcal{T}_{[X_{\hat{s}}]\xi}^n$  with  $\xi \in (0, \zeta)$  that  $\mathcal{T}_{[UX, \hat{s}]\zeta}^n(x^n) \neq \emptyset$  for  $n$  large enough. Thus by the definition in (16), it follows that  $\mathcal{T} \supset \mathcal{T}_{[X_{\hat{s}}]\xi}^n$  and thus Lemma 1.2 implies for some  $c_0 > 0$  that

$$P_{X_{\hat{s}}}^n(\mathcal{T}^c) < \exp(-nc_0). \quad (22)$$

On the other hand, for every  $x^n \in \mathcal{T}$  with  $f(x^n) = i$  and  $g(x^n) = j$ , it holds that  $(u_{ij}^n(\hat{s}), x^n) \in \mathcal{T}_{[UX, \hat{s}]\zeta}^n$ . Since for all

$s \in \mathcal{I}(\hat{s})$ , the Markov chains  $U_{\hat{s}} - X_{\hat{s}} - Y_{\hat{s}}$  hold, Lemma 1.6 implies for  $c_0$  sufficiently small that

$$P_{Y_{\hat{s}}|X_{\hat{s}}}^n(\mathcal{T}_{[UY, \hat{s}]\sigma}^n(u_{f(x^n)g(x^n)}^n(\hat{s}), x^n)|x^n) < \exp(-nc_0).$$

This inequality together with (21) and (22) gives

$$P_{XY, \hat{s}}^n(\mathcal{T}_0^c) < \exp(-nc_1), \quad (23)$$

for some  $c_1 > 0$  and  $n$  sufficiently large.

Therefore, to compute the upper-bound of the probability in (17), we may just concentrate on all  $(x^n, y^n) \in \mathcal{T}_0$  with

$$\tilde{g}(f(x^n), \hat{s}, y^n) \neq g(x^n). \quad (24)$$

A necessary condition for  $(x^n, y^n) \in \mathcal{T}_0$  is given by

$$(u_{f(x^n)g(x^n)}^n(\hat{s}), y^n) \in \bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UY, s]\sigma|\mathcal{X}}^n,$$

which together with (24) and (20) implies that

$$\exists m \neq g(x^n), (u_{f(x^n)m}^n(\hat{s}), y^n) \in \bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UY, s]\sigma|\mathcal{X}}^n. \quad (25)$$

Furthermore, it follows for all  $(x^n, y^n) \in \mathcal{T}_0$  that  $x^n \in \mathcal{T}$  and thus for  $f(x^n) = i$  and  $g(x^n) = j \neq m$ , it holds that

$$(u_{ij}^n(\hat{s}), x^n) \in \mathcal{T}_{[UX, \hat{s}]\zeta}^n. \quad (26)$$

Define the RV

$$\tilde{U}_{\hat{s}} := \{U_{ij, \hat{s}}^n\}_{(i,j) \in \mathcal{I} \times \mathcal{J}} = (U_{11, \hat{s}}^n, U_{12, \hat{s}}^n, \dots, U_{|\mathcal{I}||\mathcal{J}|, \hat{s}}^n)$$

and let  $\tilde{u}(\hat{s}) := \{u_{ij}^n(\hat{s})\}_{(i,j) \in \mathcal{I} \times \mathcal{J}}$  be an arbitrary realization. For all  $s \in \mathcal{I}(\hat{s})$  and  $(x^n, y^n) \in \mathcal{T}_0$ , the relations (25) and (26) give the following upper-bound for the error probability in (17)

$$\begin{aligned} e_s(\tilde{u}(\hat{s})) &:= \sum_{(x^n, y^n) \in \mathcal{T}_0} P_{XY, s}^n(x^n, y^n) \\ &\times \sum_{\substack{i \in \mathcal{I}, j \in \mathcal{J} \\ m \in \mathcal{J} - \{j\}}} \mathbb{1}_{\mathcal{T}_{[UX, s]\zeta}^n}(u_{ij}^n(\hat{s}), x^n) \mathbb{1}_{\bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UY, s]\sigma|\mathcal{X}}^n}(u_{im}^n(\hat{s}), y^n). \end{aligned}$$

The upper-bound of  $e_s(\tilde{u}(\hat{s}))$  is given by taking its expectation with respect to  $\tilde{U}_{\hat{s}}$  as follows

$$\begin{aligned} \mathbb{E}_{\tilde{U}_{\hat{s}}} [e_s(\tilde{U}_{\hat{s}})] &= \sum_{(x^n, y^n) \in \mathcal{T}_0} P_{XY, s}^n(x^n, y^n) \sum_{\substack{i \in \mathcal{I}, j \in \mathcal{J} \\ m \in \mathcal{J} - \{j\}}} \mathbb{E}_{(U_{ij, \hat{s}}^n, U_{im, \hat{s}}^n)} \\ &\left[ \mathbb{1}_{\mathcal{T}_{[UX, s]\zeta}^n}(U_{ij, \hat{s}}^n, x^n) \mathbb{1}_{\bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UY, s]\sigma|\mathcal{X}}^n}(U_{im, \hat{s}}^n, y^n) \right], \quad (27) \end{aligned}$$

where the equality follows by RVs  $\{U_{ij, \hat{s}}^n\}_{(i,j) \in \mathcal{I} \times \mathcal{J}}$  being independent and using the Fubini theorem [26, Chapter II, §6]. In the following, an upper-bound for the inner summation in (27) is derived, which automatically gives the upper-bound for the expectation on the left hand side.

Let  $i \in \mathcal{I}, j \in \mathcal{J}, m \in \mathcal{J} - \{j\}$  and  $\tau, \tau' > 0$  be given such that  $\delta > \tau + \tau'$ . It holds for all  $(x^n, y^n) \in \mathcal{T}_0$ , all  $\zeta, \sigma > 0$  sufficiently small, and  $n$  sufficiently large that

$$\begin{aligned} &\mathbb{E}_{(U_{ij, \hat{s}}^n, U_{im, \hat{s}}^n)} \left[ \mathbb{1}_{\mathcal{T}_{[UX, s]\zeta}^n}(U_{ij, \hat{s}}^n, x^n) \mathbb{1}_{\bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UY, s]\sigma|\mathcal{X}}^n}(U_{im, \hat{s}}^n, y^n) \right] \\ &= \Pr(U_{ij, \hat{s}}^n \in \mathcal{T}_{[UX, s]\zeta}^n(x^n)) \Pr(U_{im, \hat{s}}^n \in \bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UY, s]\sigma|\mathcal{X}}^n(y^n)) \\ &\leq |\mathcal{I}(\hat{s})| \exp \left[ -n(I(U_{\hat{s}}; X_{\hat{s}}) \right. \\ &\quad \left. + \min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) - \tau - \tau') \right], \quad (28) \end{aligned}$$

where the equality follows again by RVs  $\{U_{ij, \hat{s}}^n\}_{(i,j) \in \mathcal{I} \times \mathcal{J}}$  being independent. The inequality is a result of Lemma 1.7. Moreover, the definitions in (12) and (13) imply that

$$\begin{aligned} N_{\hat{s},1} N_{\hat{s},2} (N_{\hat{s},2} - 1) &\leq N_{\hat{s},1} N_{\hat{s},2} N_{\hat{s},2} \\ &= \exp \left[ n(I(U_{\hat{s}}; X_{\hat{s}}) + \min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) - \delta) \right]. \quad (29) \end{aligned}$$

By using (28) and (29), it follows that the inner summation in (27) is upper-bounded by  $|\mathcal{I}(\hat{s})| \exp[-n(\delta - \tau - \tau')]$ , which implies that

$$\mathbb{E}_{\tilde{U}_{\hat{s}}} [e_s(\tilde{U}_{\hat{s}})] \leq |\mathcal{I}(\hat{s})| \exp[-n(\delta - \tau - \tau')]. \quad (30)$$

Let  $\delta_1$  be sufficiently small such that  $0 < \delta_1 < \delta - \tau - \tau'$ . By the Markov inequality, it follows that

$$\Pr(e_s(\tilde{U}_{\hat{s}}) \geq \exp(-n\delta_1)) \leq \frac{\mathbb{E}_{\tilde{U}_{\hat{s}}} [e_s(\tilde{U}_{\hat{s}})]}{\exp(-n\delta_1)}. \quad (31)$$

Therefore, (30) and (31) imply for all  $\zeta$  and  $\sigma$  sufficiently small, and all  $n$  large enough that

$$\begin{aligned} &\Pr \left( \bigcap_{s \in \mathcal{I}(\hat{s})} \left\{ e_s(\tilde{U}_{\hat{s}}) < \exp(-n\delta_1) \right\} \right) \\ &\geq 1 - |\mathcal{I}(\hat{s})|^2 \exp(-n(\delta - \tau - \tau' - \delta_1)). \quad (32) \end{aligned}$$

Thus, there exists a realization  $\tilde{u}(\hat{s}) = \{u_{ij}^n(\hat{s})\}_{(i,j) \in \mathcal{I} \times \mathcal{J}}$  of the RV  $\tilde{U}_{\hat{s}}$ , where for all  $s \in \mathcal{I}(\hat{s})$  and  $(x^n, y^n) \in \mathcal{T}_0$ , the upper-bound of the error probability in (17) is given by  $\exp(-n\delta_1)$ . This implies by using (23) that the total error probability in (17) is exponentially small with some  $\delta_0 > 0$ .

b) The proof of the second part is very similar to the first part. For a given  $(i, j) \in \mathcal{I} \times \mathcal{J}$ , the number of chosen random sequences  $v_{pq}^{ij,n}$  is  $N_{\hat{s},3} N_{\hat{s},4} = \exp(nR')$ , where  $R'$  is the rate of choosing the random sequences. Similar to (19), conditions (14) and (15) imply that  $R' = I(V_{\hat{s}}; X_{\hat{s}}|U_{\hat{s}}) + \delta$ . Furthermore, as a result of Lemma 1.1, from  $(u_{ij}^n(\hat{s}), x^n) \in \mathcal{T}_{[UX, \hat{s}]\zeta}^n$  follows  $\mathcal{T}_{[UVX, \hat{s}]\sigma}^n(u_{ij}^n(\hat{s}), x^n) \neq \emptyset$ . Therefore, Lemma 3 implies that functions  $\varphi$  and  $\rho$  as mentioned in the lemma do exist.

According to part a) of this lemma, Bob is able to reconstruct  $g(x^n) = j$ , by knowing  $f(x^n), \hat{s}$  and  $y^n$ . Therefore, he knows also  $u_{ij}^n(\hat{s})$ . Let  $\vartheta \in \mathbb{R}$  be given such that  $\vartheta > \sigma$ . Similar to (20), the decoder is defined as  $\tilde{\rho}(i, j, p, \hat{s}, y^n) := q$  if

$$\begin{aligned} q &\in \mathcal{Q}, \quad v_{pq}^{ij,n}(\hat{s}) \in \bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UVY, s]\vartheta|\mathcal{X}}^n(u_{ij}^n(\hat{s}), y^n) \quad \text{and} \\ \forall r \in \mathcal{Q}, r \neq q &\Rightarrow v_{pr}^{ij,n}(\hat{s}) \notin \bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UVY, s]\vartheta|\mathcal{X}}^n(u_{ij}^n(\hat{s}), y^n), \end{aligned}$$

and otherwise zero. Define the set  $\mathcal{T}'_0$  as follows. Similar to (23), the probability  $P_{XY, s}^n(\mathcal{T}_0^c)$  is exponentially small.

$$\begin{aligned} \mathcal{T}'_0 &:= \left\{ (x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : x^n \in \mathcal{T} \right. \\ &\quad \left. \wedge (u_{f(x^n)g(x^n)}^n(\hat{s}), v_{\varphi(x^n)\rho(x^n)}^{f(x^n)g(x^n), n}(\hat{s}), x^n, y^n) \in \bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UVXY, s]\vartheta}^n \right\}. \end{aligned}$$

For a given  $(i, j) \in \mathcal{I} \times \mathcal{J}$  define  $\tilde{V}_{ij, \hat{s}} := \{V_{pq, \hat{s}}^{ij,n}\}_{(p,q) \in \mathcal{P} \times \mathcal{Q}}$  and let  $\tilde{v}_{ij}(\hat{s}) := \{v_{pq}^{ij,n}(\hat{s})\}_{(p,q) \in \mathcal{P} \times \mathcal{Q}}$  be an arbitrary realization.

Define for all  $(x^n, y^n) \in \mathcal{T}_0'$  with  $f(x^n) = i, g(x^n) = j$ ,

$$e_s(\tilde{v}_{ij}(\hat{s})) := \sum_{\substack{p \in \mathcal{P}, q \in \mathcal{Q} \\ r \in \mathcal{Q} - \{q\}}} \mathbb{1}_{\bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UVXY, s] \vartheta}^n} (u_{ij}^n(\hat{s}), v_{pq}^{ij, n}(\hat{s}), x^n, y^n) \\ \times \mathbb{1}_{\bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UVXY, s] \vartheta | \mathcal{X}}^n} (u_{ij}^n(\hat{s}), v_{pr}^{ij, n}(\hat{s}), y^n). \quad (33)$$

Similarly as in part a), it can be shown that the error probability in (18) is upper-bounded for all  $(x^n, y^n) \in \mathcal{T}_0'$  by

$$\sum_{i \in \mathcal{I}, j \in \mathcal{J}} \sum_{\substack{(x^n, y^n) \in \mathcal{T}_0' \\ f(x^n) = i, g(x^n) = j}} P_{XY, s}(x^n, y^n) e_s(\tilde{v}_{ij}(\hat{s})). \quad (34)$$

For  $\tau, \tau' > 0$  with  $\tau + \tau' < \delta$ , Lemma 1.8 implies that

$$\mathbb{E}_{(V_{pq, \hat{s}}^{ij, n}, V_{pr, \hat{s}}^{ij, n})} \left[ \mathbb{1}_{\bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UVXY, s] \vartheta}^n} (u_{ij}^n(\hat{s}), V_{pq, \hat{s}}^{ij, n}, x^n, y^n) \right. \\ \left. \times \mathbb{1}_{\bigcup_{s \in \mathcal{I}(\hat{s})} \mathcal{T}_{[UVXY, s] \vartheta | \mathcal{X}}^n} (u_{ij}^n(\hat{s}), V_{pr, \hat{s}}^{ij, n}, y^n) \mid U_{ij, \hat{s}}^n = u_{ij}^n(\hat{s}) \right] \\ \leq |\mathcal{I}(\hat{s})|^2 \cdot \exp \left[ -n \left( I(V_{\hat{s}}; X_{\hat{s}} | U_{\hat{s}}) \right. \right. \\ \left. \left. + \min_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Y_s | U_{\hat{s}}) - \tau - \tau' \right) \right]. \quad (35)$$

Moreover, by (14) and (15), it follows that

$$N_{\hat{s}, 3} N_{\hat{s}, 4} (N_{\hat{s}, 4} - 1) \leq N_{\hat{s}, 3} N_{\hat{s}, 4} N_{\hat{s}, 4} \\ = \exp \left[ n \left( I(V_{\hat{s}}; X_{\hat{s}} | U_{\hat{s}}) + \min_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Y_s | U_{\hat{s}}) - \delta \right) \right]. \quad (36)$$

Thus, (35) and (36) imply by using the definition in (33) that

$$\mathbb{E}_{\tilde{V}_{ij, \hat{s}}} \left[ e_s(\tilde{V}_{ij, \hat{s}}) \mid U_{ij, \hat{s}}^n = u_{ij}^n(\hat{s}) \right] \leq |\mathcal{I}(\hat{s})|^2 \exp \left[ -n(\delta - \tau - \tau') \right].$$

Therefore, it follows for all  $0 < \delta'_1 < \delta - \tau - \tau'$  that

$$\Pr \left( \bigcap_{s \in \mathcal{I}(\hat{s})} \left\{ e_s(\tilde{V}_{ij, \hat{s}}) < \exp(-n\delta'_1) \right\} \mid U_{ij, \hat{s}}^n = u_{ij}^n(\hat{s}) \right) \\ \geq 1 - |\mathcal{I}(\hat{s})|^3 \exp(-n(\delta - \tau - \tau' - \delta'_1)).$$

This implies that there exist sequences  $\tilde{v}_{ij}(\hat{s})$ , for which the error upper-bound in (34) is exponentially small. ■

**Lemma 8.** Let Alice's state  $\hat{s} \in \hat{\mathcal{S}}$  be given and  $C, D_s$ , and  $\hat{S}_s$  with  $s \in \mathcal{I}(\hat{s})$  be RVs taking value in  $\mathcal{C}, \mathcal{D}$ , and  $\hat{\mathcal{S}}$  respectively. RVs  $C$  and  $D_s$  denote the CR and part of Eve's Knowledge respectively. Assume  $\alpha \in (0, \frac{1}{6}]$  and  $\eta \in (0, \frac{1}{3}]$  with  $\alpha \leq \eta$  are given and for all  $s \in \mathcal{I}(\hat{s})$ , there exist sets  $\mathcal{B}_s \subset \mathcal{C} \times \mathcal{D}$  with

$$\forall (c, d) \in \mathcal{B}_s, P_{CD, s | \hat{S}_s}(c, d | \hat{s}) < (\alpha |\mathcal{B}_s|)^{-1}, \quad (37)$$

$$P_{CD, s | \hat{S}_s}(\mathcal{B}_s | \hat{s}) \geq 1 - (\eta^2 - \alpha^2). \quad (38)$$

Furthermore, define the sets  $\mathcal{B}_{s, d} := \{c \in \mathcal{C} : (c, d) \in \mathcal{B}_s\}$  and  $\mathcal{D}_s := \{d \in \mathcal{D} : \mathcal{B}_{s, d} \neq \emptyset\}$ , and assume

$$k \in \mathbb{N}, k < \alpha^6 \min_{s \in \mathcal{I}(\hat{s}), d \in \mathcal{D}_s} |\mathcal{B}_{s, d}|, k < e^{1/\alpha} (2|\mathcal{D}| |\mathcal{I}(\hat{s})|)^{-1}. \quad (39)$$

Then, there exists a SK generator  $\kappa : \mathcal{C} \rightarrow \{1, 2, \dots, k\}$  which maps the CR to a SK  $\kappa(C)$  such that for all  $s \in \mathcal{I}(\hat{s})$ ,

$$S(\kappa(C) | D_s, \hat{S}_s = \hat{s}) \leq (\alpha + 2\eta) \log k + h(\alpha + \eta), \quad (40)$$

with a probability at least  $1 - 2k |\mathcal{I}(\hat{s})| |\mathcal{D}| e^{-\frac{\alpha^5 \min_{s \in \mathcal{I}(\hat{s}), d \in \mathcal{D}_s} |\mathcal{B}_{s, d}|}{k}}$  where the min in the exponent is taken over all  $s \in \mathcal{I}(\hat{s})$  and  $d \in \mathcal{D}_s$ .

*Proof:* Let  $s \in \mathcal{I}(\hat{s})$  be given. Define:

$$\lambda := \alpha^3 \cdot \min_{s \in \mathcal{I}(\hat{s}), d \in \mathcal{D}_s} |\mathcal{B}_{s, d}|, \quad (41)$$

$$\mathcal{D}'_s := \left\{ d \in \mathcal{D} : P_{D_s | \hat{S}_s}(d | \hat{s}) \geq \frac{\alpha^2 |\mathcal{B}_{s, d}|}{|\mathcal{B}_s|} \right\}, \quad (42)$$

$$\mathcal{B}'_s := \mathcal{B}_s \cap (\mathcal{C} \times \mathcal{D}'_s), \quad (43)$$

$$\mathcal{G}_s := \left\{ (c, d) \in \mathcal{C} \times \mathcal{D} : P_{C | D \hat{S}_s}(c | d, \hat{s}) \leq \frac{1}{\lambda} \right\}, \quad (44)$$

$$\mathcal{G}_{s, d} := \left\{ c \in \mathcal{C} : (c, d) \in \mathcal{G}_s \right\}, \quad (45)$$

$$\mathcal{E}_s := \left\{ d \in \mathcal{D} : P_{C | D \hat{S}_s}(\mathcal{G}_{s, d} | d, \hat{s}) < 1 - \eta \right\}. \quad (46)$$

Similarly as in [7, Lemma 17.5], we show in the first step that the following inequality is true:

$$P_{D_s | \hat{S}_s}(\mathcal{E}_s | \hat{s}) < \eta. \quad (47)$$

This inequality is required later to show that (40) holds. For this, let  $(c, d) \in \mathcal{B}'_s$  be given and  $s \in \mathcal{I}(\hat{s})$ . It follows that

$$P_{C | D \hat{S}_s}(c | d, \hat{s}) = \frac{P_{CD, s | \hat{S}_s}(c, d | \hat{s})}{P_{D_s | \hat{S}_s}(d | \hat{s})} \leq \frac{(\alpha |\mathcal{B}_s|)^{-1}}{\alpha^2 |\mathcal{B}_{s, d}| |\mathcal{B}_s|^{-1}} \leq \frac{1}{\lambda},$$

where the first inequality follows by (37), (42), and (43) and the last one by (41). This implies by the definition in (44) that

$$\mathcal{B}'_s \subset \mathcal{G}_s. \quad (48)$$

Moreover, by (42) and (43) it holds for all  $s \in \mathcal{I}(\hat{s})$  that

$$P_{D_s | \hat{S}_s}(\mathcal{D}'_s | \hat{s}) = \sum_{d \in \mathcal{D}'_s} P_{D_s | \hat{S}_s}(d | \hat{s}) < \sum_{d \in \mathcal{D}} \frac{\alpha^2 |\mathcal{B}_{s, d}|}{|\mathcal{B}_s|} = \alpha^2, \quad (49)$$

$$P_{CD, s | \hat{S}_s}(\mathcal{B}_s \cup (\mathcal{C} \times \mathcal{D}'_s) | \hat{s}) \\ = P_{CD, s | \hat{S}_s}(\mathcal{B}_s | \hat{s}) + P_{D_s | \hat{S}_s}(\mathcal{D}'_s | \hat{s}) - P_{CD, s | \hat{S}_s}(\mathcal{B}'_s | \hat{s}). \quad (50)$$

The relations (49) and (50) together with the assumption (38) of the lemma imply that

$$P_{CD, s | \hat{S}_s}(\mathcal{B}'_s | \hat{s}) \geq P_{CD, s | \hat{S}_s}(\mathcal{B}_s | \hat{s}) - P_{D_s | \hat{S}_s}(\mathcal{D}'_s | \hat{s}) \\ \geq 1 - (\eta^2 - \alpha^2) - \alpha^2 = 1 - \eta^2. \quad (51)$$

By (48) and (51), it follows that  $P_{CD, s | \hat{S}_s}(\mathcal{G}_s | \hat{s}) \geq 1 - \eta^2$ . This implies by the definition in (45) for all  $s \in \mathcal{I}(\hat{s})$  that

$$1 - \eta^2 \leq \sum_{d \in \mathcal{D}} P_{D_s | \hat{S}_s}(d | \hat{s}) P_{C | D \hat{S}_s}(\mathcal{G}_{s, d} | d, \hat{s}) \\ < \sum_{d \in \mathcal{E}_s} P_{D_s | \hat{S}_s}(d | \hat{s}) (1 - \eta) + \sum_{d \notin \mathcal{E}_s} P_{D_s | \hat{S}_s}(d | \hat{s}) \\ = -\eta \sum_{d \in \mathcal{E}_s} P_{D_s | \hat{S}_s}(d | \hat{s}) + 1,$$

where the second inequality follows by (46). The desired relation (47) follows by simplifying this inequality.

In the second step, we show that a SK generator  $\kappa$ , satisfying (40), exists. For this, consider each member of the family of PDs  $P_{C | D \hat{S}_s}(\cdot | d, \hat{s})$  with  $d \notin \mathcal{E}_s$  and  $s \in \mathcal{I}(\hat{s})$ . Lemma 4 implies for a randomly selected SK generator  $\kappa$  that

$$\Pr \left( \left\| \kappa(P_{C | D \hat{S}_s}(\cdot | d, \hat{s})) - P_0 \right\| > 2(\alpha + \eta) \right) \leq 2ke^{-\frac{\lambda \alpha^2}{k}}, \quad (52)$$

where  $P_0(i) = 1/k$  for all  $i = 1, 2, \dots, k$ . The universal upper-bound in (52) was calculated by taking  $\epsilon = 2\alpha$  in Lemma 4 and

by the inequalities  $\alpha \leq 1/6$  and  $\eta \leq 1/3$  from the assumption of the lemma. Therefore, for the following events

$$\mathcal{A}_{s,d} := \left\{ \left\| \kappa(P_{C|D\hat{s},s}(\cdot|d,\hat{s})) - P_0 \right\| \leq 2(\alpha + \eta) \right\},$$

it follows by (41) and (52) that

$$\begin{aligned} \Pr\left(\bigcap_{s \in \mathcal{I}(\hat{s}), d \notin \mathcal{E}_s} \mathcal{A}_{s,d}\right) &\geq 1 - \sum_{s \in \mathcal{I}(\hat{s}), d \notin \mathcal{E}_s} \Pr(\mathcal{A}_{s,d}^c) \\ &\geq 1 - 2k|\mathcal{D}||\mathcal{I}(\hat{s})|e^{-\frac{\alpha^5 \min |\mathcal{B}_{s,d}|}{k}}, \end{aligned} \quad (53)$$

where the min in (53) is taken over all  $s \in \mathcal{I}(\hat{s})$  and  $d \in \mathcal{D}_s$ .

This means that a SK generator  $\kappa$  satisfies the relation  $\|\kappa(P_{C|D\hat{s},s}(\cdot|d,\hat{s})) - P_0\| \leq 2(\alpha + \eta)$  simultaneously for all  $d \notin \mathcal{E}_s$  and  $s \in \mathcal{I}(\hat{s})$  with the probability stated in (53). Therefore, it holds by the same probability that

$$\begin{aligned} S(\kappa(C)|D_s, \hat{S}_s = \hat{s}) &= \sum_{d \in \mathcal{D}} P_{D_s|\hat{S}_s}(d|\hat{s}) \left[ \log k - H(\kappa(C)|D_s = d, \hat{S}_s = \hat{s}) \right] \\ &\leq \sum_{d \notin \mathcal{E}_s} P_{D_s|\hat{S}_s}(d|\hat{s}) [(\alpha + \eta) \log k + h(\alpha + \eta)] \\ &\quad + \sum_{d \in \mathcal{E}_s} P_{D_s|\hat{S}_s}(d|\hat{s}) \log k \leq (\alpha + 2\eta) \log k + h(\alpha + \eta), \end{aligned}$$

which gives the desired relation in (40). The equality is the result of Definition 3 and the first inequality follows from the uniform continuity of entropy [24], [7, Problem 3.10]. The last step is a result of the inequality (47). Moreover, by combining the two assumptions in (39), it implies that

$$k \ln(2k|\mathcal{D}| \cdot |\mathcal{I}(\hat{s})|) < \alpha^5 \cdot \min_{s \in \mathcal{I}(\hat{s}), d \in \mathcal{D}_s} |\mathcal{B}_{s,d}|,$$

and consequently, the probability in (53) is non-zero. ■

### C. Proof of Main Results

In the following, the proofs of Theorems 1, 2, and 3 are presented. For the proof of the first two theorems, similar techniques which are used for deriving the non-compound SK capacity results in [7, Theorem 17.21], [5], are used and extended to the finite compound setup. For completeness, all proofs are presented in detail. The proof of Theorem 3 is based on an approximation technique and uses Lemmas 5 and 6.

*Proof of Theorem 1:* Let  $\delta > 0$ , and  $0 < \xi < \zeta < \sigma$ , all in  $\mathbb{R}$  be given. For each  $\hat{s} \in \hat{\mathcal{S}} = \{\hat{s}_1, \dots, \hat{s}_m\}$ , let  $U_{\hat{s}}$  and  $V_{\hat{s}}$  satisfy for all  $s \in \mathcal{I}(\hat{s})$  the Markov chains  $U_{\hat{s}} - V_{\hat{s}} - X_{\hat{s}} - Y_s Z_s$ .

Consider  $N_{\hat{s},1}N_{\hat{s},2}$  sequences  $u_{ij}^n(\hat{s}) \in \mathcal{U}^n$  as given in Table I, which are chosen independently by PD  $P_{U_{\hat{s}}}^n$  with

$$i \in \mathcal{I} := \{1, 2, \dots, N_{\hat{s},1}\}, \quad j \in \mathcal{J} := \{1, 2, \dots, N_{\hat{s},2}\},$$

and  $N_{\hat{s},1}$  and  $N_{\hat{s},2}$  satisfying (12) and (13) from Lemma 7. Moreover, for every  $u_{ij}^n(\hat{s})$  from Table I, consider  $N_{\hat{s},3}N_{\hat{s},4}$  sequences  $v_{pq}^{ij,n}(\hat{s}) \in \mathcal{V}^n$ , which are chosen conditionally independently by PD  $P_{V_{\hat{s}}|U_{\hat{s}}}^n(\cdot|u_{ij}^n(\hat{s}))$  with

$$p \in \mathcal{P} := \{1, 2, \dots, N_{\hat{s},3}\}, \quad q \in \mathcal{Q} := \{1, 2, \dots, N_{\hat{s},4}\},$$

and  $N_{\hat{s},3}$  and  $N_{\hat{s},4}$  satisfying (14) and (15) from Lemma 7. Assume that the random sequences  $u_{ij}^n(\hat{s})$  in Table I and their

$\hat{s}_1$	$u_{11}^n(\hat{s}_1)$	$\dots$	$u_{ij}^n(\hat{s}_1)$	$\dots$	$u_{N_{\hat{s}_1,1}N_{\hat{s}_1,2}}^n(\hat{s}_1)$
$\vdots$	$\vdots$		$\vdots$		$\vdots$
$\hat{s}_m$	$u_{11}^n(\hat{s}_m)$	$\dots$	$u_{ij}^n(\hat{s}_m)$	$\dots$	$u_{N_{\hat{s}_m,1}N_{\hat{s}_m,2}}^n(\hat{s}_m)$

Table I: Random sequences for a DMMS with  $|\hat{\mathcal{S}}| = m$

corresponding sequences  $\{v_{pq}^{ij,n}(\hat{s})\}_{(p,q) \in \mathcal{P} \times \mathcal{Q}}$  are known to Alice and Bob.

To show the achievability of (6), the proof is divided into two parts. In part a), the following rate is shown to be achievable:

$$R'_{\text{sk}} := \min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) - \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Z_s), \quad (54)$$

when  $R'_{\text{sk}}$  is positive and RV  $U_{\hat{s}}$  satisfies for all  $s \in \mathcal{I}(\hat{s})$

$$U_{\hat{s}} - X_{\hat{s}} - Y_s Z_s \quad \text{and} \quad \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; X_{\hat{s}}|Y_s) < \Gamma. \quad (55)$$

This gives a special case of (6) and (7). In part b), the achievability of the SK rate in (6) is shown, when it is positive.

*Part a)* Assume  $R'_{\text{sk}}$  from (54) is positive i.e.

$$\min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) > \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Z_s). \quad (56)$$

As explained in Section III, Alice estimates her marginal statistic by hypothesis testing. Assume that  $\hat{s} \in \hat{\mathcal{S}}$  is the index corresponding to the correct decision and all other  $\tilde{s} \in \hat{\mathcal{S}} - \{\hat{s}\}$  correspond to a wrong decision. For any observation  $X_{\hat{s}}^n$ , let the resulting estimated state be denoted by the RV  $\hat{S}_{\hat{s}}$ , taking value in the set  $\hat{\mathcal{S}}$  and having the PD  $P_{\hat{S}_{\hat{s}}}$ . It holds by [21] and [7, Problem 2.13b] for some  $c_0, c_1 > 0$  that

$$P_{\hat{S}_{\hat{s}}}(\hat{s}) \geq 1 - \exp(-nc_0), \quad (57)$$

$$\forall \tilde{s} \in \hat{\mathcal{S}} - \{\hat{s}\}, P_{\hat{S}_{\hat{s}}}(\tilde{s}) \leq \exp(-nc_1). \quad (58)$$

Next, Alice sends her estimated marginal source state to Bob over the public noiseless channel. Assume that the hypothesis testing has led to the correct decision  $\hat{s}$ . Alice and Bob find the corresponding family of sequences  $\{u_{ij}^n(\hat{s})\}_{(i,j) \in \mathcal{I} \times \mathcal{J}}$  from Table I by knowing  $\hat{s}$ . Lemma 7a implies the existence of the encoder functions  $f: \mathcal{X}^n \rightarrow \mathcal{I} \cup \{0\}$  and  $g: \mathcal{X}^n \rightarrow \mathcal{J} \cup \{0\}$ . These encoders give the indices  $f(x^n) = i$  and  $g(x^n) = j$  of the sequence  $u_{ij}^n(\hat{s})$  to be chosen from the family of sequences  $\{u_{ij}^n(\hat{s})\}_{(i,j) \in \mathcal{I} \times \mathcal{J}}$ .

As shown in Figure 2, in addition to the transmitted  $\hat{s}$ , Alice sends further the index  $f(x^n) = i$  to Bob over the public channel. Lemma 7a implies the existence of a decoder  $\tilde{g}: \mathcal{I} \times \hat{\mathcal{S}} \times \mathcal{Y}^n \rightarrow \mathcal{J}$ , with which, Bob can reconstruct the index  $g(x^n) = j$ . This  $j$  is the CR between Alice and Bob.

In total, for all Alice's estimation results which may lead to a correct or incorrect decision, the error probability upper-bound for all  $s \in \mathcal{I}(\hat{s})$  is given by

$$\begin{aligned} &\Pr\{g(X_{\hat{s}}^n) \neq \tilde{g}(f(X_{\hat{s}}^n), \hat{S}_{\hat{s}}, Y_s^n)\} \\ &= \Pr\{g(X_{\hat{s}}^n) \neq \tilde{g}(f(X_{\hat{s}}^n), \hat{s}, Y_s^n) \wedge \hat{S}_{\hat{s}} = \hat{s}\} \\ &\quad + \sum_{\tilde{s} \in \hat{\mathcal{S}} - \{\hat{s}\}} P_{\hat{S}_{\hat{s}}}(\tilde{s}) \Pr\{g(X_{\hat{s}}^n) \neq \tilde{g}(f(X_{\hat{s}}^n), \hat{S}_{\hat{s}}, Y_s^n) \mid \hat{S}_{\hat{s}} = \tilde{s}\} \\ &\leq \exp(-n\delta_0) + \exp(-nc_1) \cdot |\hat{\mathcal{S}}|, \end{aligned} \quad (59)$$



where the inequality is a result of (17) for some  $\delta_0 > 0$  and (58). Thus, condition (3) of Definition 4 is satisfied.

The whole message which is sent over the public channel is represented by the RV  $f_c(X_s^n) = (f(X_s^n), \hat{S}_s)$  having the range size  $\|f\| \cdot |\hat{S}|$ . As shown in the following, the communication rate satisfies condition (1) of Definition 4:

$$\begin{aligned} \frac{1}{n} \log \|f_c\| &= \frac{1}{n} \log(\|f\| \cdot |\hat{S}|) = \frac{1}{n} \log(N_{\hat{S},1} \cdot |\hat{S}|) \\ &= \max_{s \in \mathcal{I}(\hat{s})} I(U_s; X_s | Y_s) + 3\delta + \frac{1}{n} \log |\hat{S}| < \Gamma + 3\delta, \end{aligned}$$

where the last equality follows by (12) and the inequality is a result of (55) and is valid for all  $n$  sufficiently large.

After the index  $g(x^n) = j$  is reconstructed by Bob, both Alice and Bob may generate their SK, based on this CR. Thus, it remains to show that there exists a SK generator  $\kappa : \mathcal{J} \rightarrow \{1, 2, \dots, k\}$ , giving rise to the RV  $K_A = \kappa(g(X_s^n))$ , which satisfies condition (4) of Definition 4.

Again the condition is verified for both estimation results. Assume hypothesis testing has led to the correct decision and  $\hat{s}$  is sent to Bob over the public channel. Define for  $s \in \mathcal{I}(\hat{s})$

$$\mathcal{T}_s := \left\{ (x^n, z^n) \in \mathcal{X}^n \times \mathcal{Z}^n : x^n \in \mathcal{T} \wedge (u_{f(x^n)g(x^n)}^n(\hat{s}), x^n, z^n) \in \mathcal{T}_{[UXZ,s]\sigma}^n \right\},$$

where  $\mathcal{T}$  is given in (16). A similar discussion as for (23) from Lemma 7, implies for some  $c_2 > 0$  and  $n$  large enough that

$$P_{XZ,s}^n(\mathcal{T}_s^c) < \exp(-nc_2). \quad (60)$$

Similarly as in [7, Theorem 17.21] for the non-compound version, define for all  $s \in \mathcal{I}(\hat{s})$ , the RVs  $C$  and  $D_s$  and the set  $\mathcal{B}_s$  to be used in Lemma 8, as follows

$$\begin{aligned} C &:= g(X_s^n), & D_s &:= (f(X_s^n), Z_s^n, \mathbb{1}_{\mathcal{T}_s}(X_s^n, Z_s^n)), \\ \mathcal{B}_s &:= \left\{ (j, (i, z^n, 1)) : (i, j) \in \mathcal{I} \times \mathcal{J}, z^n \in \mathcal{T}_{[Z_s]\xi}^n, \right. \\ &\quad \left. \mathcal{T}_{[UXZ,s]\sigma}^n(u_{ij}^n(\hat{s}), z^n) \neq \emptyset \right\}. \end{aligned} \quad (61)$$

Assume, RVs  $C$  and  $D_s$  take their values in the sets  $\mathcal{C}$  and  $\mathcal{D}$  respectively. Moreover, the sets  $\mathcal{D}_s$  and  $\mathcal{B}_{s,d}$  are defined as in Lemma 8. In the following, it will be shown that all conditions of Lemma 8 are satisfied. It holds that

$$\begin{aligned} P_{CD,s|\hat{s}}(\mathcal{B}_s|\hat{s}) &= \sum_{(j,(i,z^n,1)) \in \mathcal{B}_s} P_{CD,s|\hat{s}}(j, (i, z^n, 1)|\hat{s}) \\ &= \sum_{(j,(i,z^n,1)) \in \mathcal{B}_s} \sum_{\substack{x^n: f(x^n)=i, g(x^n)=j, \\ \mathbb{1}_{\mathcal{T}_s}(x^n, z^n)=1}} P_{X_s^n Z_s^n|\hat{s}}(x^n, z^n|\hat{s}) \\ &= P_{X_s^n Z_s^n|\hat{s}} \left( \mathcal{T}_s \cap \left\{ (x^n, z^n) \in \mathcal{X}^n \times \mathcal{Z}^n : z^n \in \mathcal{T}_{[Z_s]\xi}^n \right\} \middle| \hat{s} \right) \\ &\geq 1 - \left[ P_{X_s^n Z_s^n|\hat{s}}(\mathcal{T}_s^c|\hat{s}) + P_{Z_s^n|\hat{s}}(\mathcal{T}_{[Z_s]\xi}^n|\hat{s}) \right] \\ &\geq 1 - \frac{P_{X_s^n Z_s^n}(\mathcal{T}_s^c) + P_{Z_s^n}(\mathcal{T}_{[Z_s]\xi}^n)}{1 - \exp(-nc_0)} \geq 1 - \exp(-nc_3), \end{aligned} \quad (62)$$

for some  $c_3 > 0$  and  $n$  sufficiently large. The last two inequalities follow by (57), (60) and Lemma 1.2.

Furthermore, define the parameters  $\alpha$  and  $\eta$  for some arbitrary  $\tau > 0$  as follows

$$\alpha := \exp(-n(\delta + 5\tau)), \quad \eta := \exp(-n\delta). \quad (63)$$

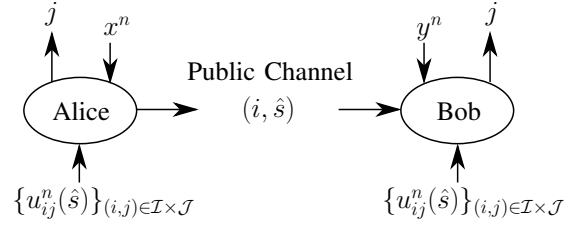


Fig. 2: Generating the CR  $j$

For  $\delta$  and  $\tau$  sufficiently small and  $n$  large enough, it holds that  $\eta^2 - \alpha^2 > \exp(-nc_3)$ . Therefore, it follows by (62) that

$$P_{CD,s|\hat{s}}(\mathcal{B}_s|\hat{s}) \geq 1 - (\eta^2 - \alpha^2).$$

This guarantees condition (38) of Lemma 8. Moreover, the conditions  $\alpha \in (0, 1/6]$  and  $\eta \in (0, 1/3]$  are also satisfied.

To check condition (37) of Lemma 8, we find first an upper-bound of  $|\mathcal{B}_s|$ . The non-emptiness constraint  $\mathcal{T}_{[UXZ,s]\sigma}^n(u_{ij}^n(\hat{s}), z^n) \neq \emptyset$  from the definition of the set  $\mathcal{B}_s$  is a sufficient condition for  $u_{ij}^n(\hat{s}) \in \mathcal{T}_{[UZ,s]\sigma|\mathcal{X}}^n(z^n)$  and thus

$$|\mathcal{B}_s| \leq \sum_{z^n \in \mathcal{T}_{[Z_s]\xi}^n} \left| \left\{ (i, j) \in \mathcal{I} \times \mathcal{J} : u_{ij}^n(\hat{s}) \in \mathcal{T}_{[UZ,s]\sigma|\mathcal{X}}^n(z^n) \right\} \right|. \quad (64)$$

Furthermore, for  $R$  being the rate of choosing the random sequences  $\{u_{ij}^n(\hat{s})\}_{(i,j) \in \mathcal{I} \times \mathcal{J}}$ , it holds by (12) and (13) that

$$\begin{aligned} R &= \max_{s \in \mathcal{I}(\hat{s})} I(U_s; X_s | Y_s) + \min_{s \in \mathcal{I}(\hat{s})} I(U_s; Y_s) + \delta \\ &> \min_{s \in \mathcal{I}(\hat{s})} I(U_s; Y_s) > \max_{s \in \mathcal{I}(\hat{s})} I(U_s; Z_s), \end{aligned}$$

where the last inequality is the result of the assumption (56). Moreover, for all  $(j, (i, z^n, 1)) \in \mathcal{B}_s$  it holds that  $z^n \in \mathcal{T}_{[Z_s]\xi}^n$  which implies by using Lemma 1.1 for  $n$  large enough that  $\mathcal{T}_{[UXZ,s]\sigma}^n(u_{ij}^n(\hat{s}), z^n) \neq \emptyset$ . Therefore, it follows by (64) and Lemma 2 for  $\xi$  and  $\zeta$  sufficiently small and  $n$  large enough that

$$\begin{aligned} |\mathcal{B}_s| &\leq |\mathcal{T}_{[Z_s]\xi}^n| \exp \left[ n(R - I(U_s; Z_s) + \tau) \right] \\ &\leq \exp \left[ n(H(Z_s) + \tau) \right] \\ &\quad \times \exp \left[ n(I(U_s; X_s) + \delta - I(U_s; Z_s) + \tau) \right], \end{aligned} \quad (65)$$

where the last inequality follows by (19) and Lemma 1.4.

In the second step of verifying condition (37), we find an upper-bound for  $P_{CD,s|\hat{s}}(j, (i, z^n, 1)|\hat{s})$ . For all  $(j, (i, z^n, 1)) \in \mathcal{B}_s$ , it holds by using (57) and (61) that

$$\begin{aligned} &(1 - \exp(-nc_0)) \cdot P_{CD,s|\hat{s}}(j, (i, z^n, 1)|\hat{s}) \\ &\leq P_{CD,s}(j, (i, z^n, 1)) \\ &\leq \sum_{x^n \in \mathcal{T}_{[UXZ,s]\sigma}^n(u_{ij}^n(\hat{s}), z^n)} P_{XZ,s}^n(x^n, z^n) \\ &\leq |\mathcal{T}_{[UXZ,s]\sigma}^n(u_{ij}^n(\hat{s}), z^n)| \exp \left[ -n(H(X_s Z_s) - \tau) \right] \\ &\leq \exp \left[ n(H(X_s | U_s Z_s) - H(X_s Z_s) + 2\tau) \right], \end{aligned} \quad (66)$$

where the third inequality follows by Lemma 1.3 and the last one by Lemma 1.5 for  $\sigma$  sufficiently small and  $n$  large enough.

Moreover, by using Markov chains in (55), it holds that

$$\begin{aligned} H(X_{\hat{s}}|U_{\hat{s}}Z_s) - H(X_{\hat{s}}Z_s) \\ = -I(U_{\hat{s}}; X_{\hat{s}}) - H(Z_s) + I(U_{\hat{s}}; Z_s). \end{aligned} \quad (67)$$

The relations (65), (66), and (67) together with the definition of  $\alpha$  in (63) imply for  $n$  large enough that

$$|\mathcal{B}_s| P_{CD,s|\hat{S}_s}(j, (i, z^n, 1)|\hat{s}) \alpha \leq \frac{\exp(-n\tau)}{1 - \exp(-nc_0)} < 1.$$

Thus, condition (37) of Lemma 8 is also satisfied.

Therefore, Lemma 8 implies that there exists a SK generator  $\kappa : \mathcal{J} \rightarrow \{1, 2, \dots, k\}$  with  $k$  satisfying (39), such that the relation (40) holds. By the definitions in (63), both  $\alpha$  and  $\eta$  approach zero exponentially fast. Moreover, by (39) and (65), it follows that  $k$  does not increase faster than exponentially. Thus, the inequality (40) implies for  $K_A = \kappa(g(X_{\hat{s}}^n))$  that

$$\begin{aligned} S(K_A | f(X_{\hat{s}}^n), Z_s^n, \mathbb{1}_{\mathcal{T}_s}(X_{\hat{s}}^n, Z_s^n), \hat{S}_s = \hat{s}) \\ \leq (\alpha + 2\eta) \log k + h(\alpha + \eta) \\ \leq n \cdot \exp(-nc_4) + \exp(-nc_4) \leq \exp(-nc_5), \end{aligned} \quad (68)$$

for some  $c_4, c_5 > 0$ . Consequently, the security index is exponentially small for the case of correct estimation decision.

In total, for all estimation results which may lead to a correct or incorrect decision, the security index is upper-bounded as shown in the following

$$\begin{aligned} S(K_A | f(X_{\hat{s}}^n), Z_s^n, \mathbb{1}_{\mathcal{T}_s}(X_{\hat{s}}^n, Z_s^n), \hat{S}_s) \\ = P_{\hat{S}_s}(\hat{s}) S(K_A | Z_s^n, f(X_{\hat{s}}^n), \mathbb{1}_{\mathcal{T}_s}(X_{\hat{s}}^n, Z_s^n), \hat{S}_s = \hat{s}) \\ + \sum_{\tilde{s} \in \hat{\mathcal{S}} - \{\hat{s}\}} P_{\hat{S}_s}(\tilde{s}) S(K_A | Z_s^n, f(X_{\hat{s}}^n), \mathbb{1}_{\mathcal{T}_s}(X_{\hat{s}}^n, Z_s^n), \hat{S}_s = \tilde{s}) \\ \leq \exp(-nc_5) + n \cdot \exp(-nc_6) \cdot |\hat{\mathcal{S}}|, \end{aligned}$$

for some  $c_6 > 0$ . The last inequality is a result of (58) and (68) and the fact that  $k$  does not increase faster than exponentially. Therefore, condition (4) of Definition 4 is satisfied.

In the rest of this part, we show that  $R'_{\text{sk}}$  satisfies condition (2) of Definition 4. By using the definition of  $\alpha$  from (63) and the set  $\mathcal{D}$  being the alphabet of RV  $D_s$ , it follows that the expression  $e^{1/\alpha} (2|\mathcal{D}| |\mathcal{I}(\hat{s})|)^{-1}$  from (39) increases doubly exponentially fast. For any  $d := (i, z^n, 1) \in \mathcal{D}_s$  and  $\mathcal{B}_{s,d}$  from Lemma 8, it follows by (65) that  $|\mathcal{B}_{s,d}|$  does not increase faster than exponentially. Therefore, for  $n$  large enough, it holds that

$$\alpha^6 \cdot \min_{s \in \mathcal{I}(\hat{s}), d \in \mathcal{D}_s} |\mathcal{B}_{s,d}| < e^{1/\alpha} (2|\mathcal{D}| |\mathcal{I}(\hat{s})|)^{-1}. \quad (69)$$

Thus, to guarantee condition (39) of Lemma 8 it is necessary that  $k$  be lower than the left hand side of (69). For this, a lower-bound for  $\min_{s \in \mathcal{I}(\hat{s}), d \in \mathcal{D}_s} |\mathcal{B}_{s,d}|$  should be first determined. Lemma 1.1 implies that  $u_{ij}^n(\hat{s}) \in \mathcal{T}_{[UZ,s]\zeta}^n(z^n)$  is a sufficient condition for  $\mathcal{T}_{[UXZ,s]\sigma}^n(u_{ij}^n(\hat{s}), z^n) \neq \emptyset$ . Therefore for all  $s \in \mathcal{I}(\hat{s})$  and  $d = (i, z^n, 1) \in \mathcal{D}_s$ , it holds that

$$|\mathcal{B}_{s,d}| \geq \left| \left\{ j \in \mathcal{J} : u_{ij}^n(\hat{s}) \in \mathcal{T}_{[UZ,s]\zeta}^n(z^n) \right\} \right|. \quad (70)$$

Furthermore by using (13), the rate of choosing the random sequences  $u_{ij}^n(\hat{s})$  for a fixed index  $i$ , is given by

$$R_2 = \min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) - 2\delta. \quad (71)$$

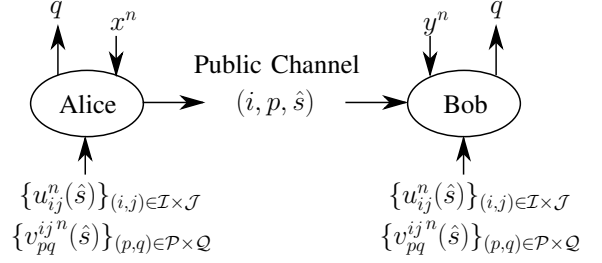


Fig. 3: Generating the CR  $q$

Thus, for  $\delta$  sufficiently small, assumption (56) gives

$$R_2 > \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Z_s). \quad (72)$$

Moreover, in deriving the inequality (65), it was shown that for all  $(j, d) = (j, (i, z^n, 1)) \in \mathcal{B}_s$ , it holds that  $\mathcal{T}_{[UZ,s]\zeta}^n(z^n) \neq \emptyset$ . Thus, Lemma 2 together with (70), (71), and (72) implies that

$$\begin{aligned} \min_{s \in \mathcal{I}(\hat{s}), d \in \mathcal{D}_s} |\mathcal{B}_{s,d}| &\geq \min_{s \in \mathcal{I}(\hat{s}), d \in \mathcal{D}_s} \left| \left\{ j : u_{ij}^n(\hat{s}) \in \mathcal{T}_{[UZ,s]\zeta}^n(z^n) \right\} \right| \\ &\geq \exp \left[ n \left( R_2 - \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Z_s) - \tau \right) \right] \\ &\geq \exp \left[ n \left( \min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) - \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Z_s) - 2\delta - \tau \right) \right]. \end{aligned}$$

Therefore, by keeping  $k$  lower than the left hand side of (69), it follows by (63) and (54) that  $\frac{1}{n} \log |\mathcal{K}| > R'_{\text{sk}} - 8\delta$ . This satisfies condition (2) of Definition 4.

*Part b)* In this part, it is shown that if

$$R_{\text{sk}} := \min_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Y_s | U_{\hat{s}}) - \max_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Z_s | U_{\hat{s}}) > 0,$$

then  $R_{\text{sk}}$  is achievable for all RVs  $U_{\hat{s}}$  and  $V_{\hat{s}}$  satisfying (7). It may be assumed that

$$\min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) \leq \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Z_s). \quad (73)$$

Because otherwise, it follows by Markov chains in (7) that

$$\begin{aligned} R_{\text{sk}} &= \min_{s \in \mathcal{I}(\hat{s})} \left[ I(V_{\hat{s}}; Y_s) + I(U_{\hat{s}}; Y_s | V_{\hat{s}}) - I(U_{\hat{s}}; Y_s) \right] \\ &\quad - \max_{s \in \mathcal{I}(\hat{s})} \left[ I(V_{\hat{s}}; Z_s) + I(U_{\hat{s}}; Z_s | V_{\hat{s}}) - I(U_{\hat{s}}; Z_s) \right] \\ &\leq \min_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Y_s) - \max_{s \in \mathcal{I}(\hat{s})} I(V_{\hat{s}}; Z_s) \\ &\quad - \left[ \min_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Y_s) - \max_{s \in \mathcal{I}(\hat{s})} I(U_{\hat{s}}; Z_s) \right], \end{aligned}$$

which implies by using part a) that  $R_{\text{sk}}$  is achievable.

Similarly as in part a), Alice sends her estimated marginal source state to Bob over the public noiseless channel. For the case that hypothesis testing has led to the correct decision  $\hat{s}$ , both Alice and Bob find the corresponding family of sequences  $\{u_{ij}^n(\hat{s})\}_{(i,j) \in \mathcal{I} \times \mathcal{J}}$  from Table I and also the related families of sequences  $\{v_{pq}^{ij,n}(\hat{s})\}_{(p,q) \in \mathcal{P} \times \mathcal{Q}}$  for each member of the chosen row of the table. Lemma 7b implies the existence of the encoder functions  $\varphi : \mathcal{X}^n \rightarrow \mathcal{P} \cup \{0\}$  and  $\rho : \mathcal{X}^n \rightarrow \mathcal{Q} \cup \{0\}$ . These encoders give the indices  $\varphi(x^n) = p$  and  $\rho(x^n) = q$  of the sequence  $v_{pq}^{ij,n}(\hat{s})$  to be chosen from the family of sequences  $\{v_{pq}^{ij,n}(\hat{s})\}_{(p,q) \in \mathcal{P} \times \mathcal{Q}}$  for given indices  $i$  and  $j$ .

As shown in Figure 3, in addition to the transmitted  $\hat{s}$ , Alice sends further the indices  $f(x^n) = i$  and  $\varphi(x^n) = p$  to Bob over the public channel. By part a) of this theorem,  $g(x^n) = j$  is known to Bob. Lemma 7b implies the existence of a decoder  $\tilde{\rho} : \mathcal{I} \times \mathcal{J} \times \mathcal{P} \times \hat{\mathcal{S}} \times \mathcal{Y}^n \rightarrow \mathcal{Q}$ , with which Bob can reconstruct the index  $q$  to be used as the CR. The upper-bound of the error probability was given in (18) from Lemma 7. Due to (73), the index  $g(x^n) = j$  can not be used as the CR any more.

Similarly as in (59) from part a), for all estimation results which may lead to a correct or incorrect decision, the error probability upper-bound for all  $s \in \mathcal{I}(\hat{s})$  is exponentially small. Therefore, condition (3) of Definition 4 is satisfied.

The public communication function is represented by the RV  $f_c(X_s^n) = (f(X_s^n), \varphi(X_s^n), \hat{S}_s)$ . As shown in the following, the communication rate satisfies condition (1) of Definition 4:

$$\begin{aligned} \frac{1}{n} \log(\|f\| \cdot \|\varphi\| \cdot |\hat{S}|) &= \max_{s \in \mathcal{I}(\hat{s})} I(U_s; X_s | Y_s) + \\ &\max_{s \in \mathcal{I}(\hat{s})} I(V_s; X_s | U_s Y_s) + 6\delta + \frac{1}{n} \log |\hat{S}| < \Gamma + 6\delta, \end{aligned}$$

for  $n$  sufficiently large. The equality is a result of (12) and (14) from Lemma 7 and the inequality follows by (7).

For showing that conditions (2) and (4) of Definition 4 also hold, the RVs  $C, D_s$ , and the set  $\mathcal{B}_s$  can be defined similarly as in part a), but this time for the coding scheme from Lemma 7b). It can be shown that conditions (37) and (38) of Lemma 8 are again satisfied and thus there exists a SK generator  $\kappa : \mathcal{Q} \rightarrow \{1, 2, \dots, k\}$ , giving rise to the RV  $K = \kappa(\rho(X_s^n))$ , which satisfies conditions (2) and (4) of Definition 4. The proof follows by a similar discussion as in part a) of this theorem for compound sources. The non-compound version is available in [7, Theorem 17.21]. ■

*Proof of Theorem 2:* For the direct part of the proof, replace  $X_s, Y_s$ , and  $Z_s$  in Theorem 1 with  $X_s^n, Y_s^n$ , and  $Z_s^n$  respectively, for arbitrary  $n \in \mathbb{N}$ ,  $\hat{s} \in \hat{\mathcal{S}}$ , and  $s \in \mathcal{I}(\hat{s})$ . This implies that the SK rate

$$\frac{1}{n} \min_{\hat{s} \in \hat{\mathcal{S}}} \max_{U_s, V_s} \left\{ \min_{s \in \mathcal{I}(\hat{s})} I(V_s; Y_s^n | U_s) - \max_{s \in \mathcal{I}(\hat{s})} I(V_s; Z_s^n | U_s) \right\}$$

is achievable for any  $n \in \mathbb{N}$ , where the outer max is taken over all RVs  $U_s$  and  $V_s$  satisfying (9).

To show the achievability of (8), we have to show that the limit in (8) exists. Similarly as in [16], the proof follows by using the Fekete's lemma [27] which states that if a sequence  $a_n$  is superadditive i.e.  $a_{n+m} \geq a_n + a_m$ , then  $\lim_{n \rightarrow \infty} a_n/n$  exists. Define the sequences

$$\begin{aligned} a_n(\hat{s}) &:= \max_{U_s, V_s} \left\{ \min_{s \in \mathcal{I}(\hat{s})} I(V_s; Y_s^n | U_s) - \max_{s \in \mathcal{I}(\hat{s})} I(V_s; Z_s^n | U_s) \right\}, \\ a_n &:= \min_{\hat{s} \in \hat{\mathcal{S}}} a_n(\hat{s}). \end{aligned} \quad (74)$$

Take two arbitrary independent Markov chains

$$U_{s,1} - V_{s,1} - X_{s,1}^n - Y_{s,1}^n Z_{s,1}^n, \quad (75)$$

$$U_{s,2} - V_{s,2} - X_{s,2}^n - Y_{s,2}^n Z_{s,2}^n, \quad (76)$$

such that  $m, n \in \mathbb{N}$  and it holds:

$$\begin{aligned} \hat{U}_s &:= (U_{s,1}, U_{s,2}), \quad \hat{V}_s := (V_{s,1}, V_{s,2}), \quad X_s^{n+m} := (X_{s,1}^n, X_{s,2}^n), \\ Y_s^{n+m} &:= (Y_{s,1}^n, Y_{s,2}^n), \quad Z_s^{n+m} := (Z_{s,1}^n, Z_{s,2}^n). \end{aligned}$$

As the two Markov chains are independent, any RV from (75) is independent of all RVs in (76) and vice versa. Therefore, the Markov chain  $\hat{U}_s - \hat{V}_s - X_s^{n+m} - Y_s^{n+m} Z_s^{n+m}$  holds and

$$\begin{aligned} a_{n+m}(\hat{s}) &= \max_{\hat{U}_s, \hat{V}_s} \left\{ \min_{s \in \mathcal{I}(\hat{s})} I(\hat{V}_s; Y_s^{n+m} | \hat{U}_s) - \max_{s \in \mathcal{I}(\hat{s})} I(\hat{V}_s; Z_s^{n+m} | \hat{U}_s) \right\} \\ &\geq \max_{\hat{U}_s, \hat{V}_s} \left\{ \min_{s \in \mathcal{I}(\hat{s})} I(V_{s,1}; Y_{s,1}^n | U_{s,1}) - \max_{s \in \mathcal{I}(\hat{s})} I(V_{s,1}; Z_{s,1}^n | U_{s,1}) \right. \\ &\quad \left. + \min_{s \in \mathcal{I}(\hat{s})} I(V_{s,2}; Y_{s,2}^n | U_{s,2}) - \max_{s \in \mathcal{I}(\hat{s})} I(V_{s,2}; Z_{s,2}^n | U_{s,2}) \right\} \\ &= a_n(\hat{s}) + a_m(\hat{s}). \end{aligned}$$

Thus, by taking the minimum from both sides of this inequality and using the definition in (74), it follows that

$$\begin{aligned} a_{n+m} &\geq \min_{\hat{s} \in \hat{\mathcal{S}}} \{a_n(\hat{s}) + a_m(\hat{s})\} \\ &\geq \min_{\hat{s} \in \hat{\mathcal{S}}} \{a_n(\hat{s})\} + \min_{\hat{s} \in \hat{\mathcal{S}}} \{a_m(\hat{s})\} = a_n + a_m. \end{aligned}$$

Therefore, the limit in (8) exists and is achievable.

For the converse, let  $R_{\text{sk}} > 0$  be an achievable SK rate and  $s \in \mathcal{S}$  be given. Assume that  $\hat{s} \in \hat{\mathcal{S}}$  is the state of the marginal RV  $X$  and thus  $s \in \mathcal{I}(\hat{s})$ . Alice sends a message  $f_c(X_s^n)$  to Bob over the public channel and generates a SK represented by RV  $K = K_A$ . It holds by Definition 3 and condition (4) of Definition 4, that for all  $\delta > 0$  and  $n$  sufficiently large,

$$\frac{1}{n} \log |\mathcal{K}| - \frac{1}{n} \min_{s \in \mathcal{I}(\hat{s})} H(K_A | Z_s^n, f_c(X_s^n)) < \delta. \quad (77)$$

Moreover, by the Fano's inequality, it holds that

$$\frac{1}{n} \max_{s \in \mathcal{I}(\hat{s})} H(K_A | Y_s^n, f_c(X_s^n)) < \frac{1}{n} \delta \log |\mathcal{K}| + \frac{1}{n}. \quad (78)$$

By adding (77) and (78), it follows that

$$\begin{aligned} \frac{1}{n} \log |\mathcal{K}| &< \frac{1}{n} \left[ \min_{s \in \mathcal{I}(\hat{s})} H(K_A | Z_s^n, f_c(X_s^n)) \right. \\ &\quad \left. - \max_{s \in \mathcal{I}(\hat{s})} H(K_A | Y_s^n, f_c(X_s^n)) \right] + \frac{1}{n} \delta \log |\mathcal{K}| + \frac{1}{n} + \delta. \end{aligned}$$

Thus, by using condition (2) of Definition 4, it follows for  $\epsilon = \delta/(1-\delta) + (n(1-\delta))^{-1} + \delta$ , and  $n$  sufficiently large that

$$\begin{aligned} R_{\text{sk}} < \frac{1}{n} \log |\mathcal{K}| + \delta \leq \frac{1}{1-\delta} \cdot \frac{1}{n} \left[ \min_{s \in \mathcal{I}(\hat{s})} I(K_A; Y_s^n | f_c(X_s^n)) \right. \\ &\quad \left. - \max_{s \in \mathcal{I}(\hat{s})} I(K_A; Z_s^n | f_c(X_s^n)) \right] + \epsilon, \end{aligned}$$

where the last inequality follows by adding and subtracting the term  $H(K_A | f_c(X_s^n))$ .

Set RVs  $U_s := f_c(X_s^n)$  and  $V_s := (f_c(X_s^n), K_A)$ . It holds that  $I(X_s^n; U_s | V_s) = 0$ . Furthermore, as  $f_c(X_s^n)$  and  $K_A$  are both functions of  $X_s^n$ , it implies that  $I(Y_s^n, Z_s^n; U_s V_s | X_s^n) = 0$ . This proves that the Markov chains in (9) are valid.

Finally, by taking the maximum with respect to  $U_s$  and  $V_s$  and the minimum with respect to  $\hat{s} \in \hat{\mathcal{S}}$ , it follows for  $\delta > 0$  sufficiently small and  $n$  large enough that

$$R_{\text{sk}} \leq \frac{1}{n} \min_{\hat{s} \in \hat{\mathcal{S}}} \max_{U_s, V_s} \left[ \min_{s \in \mathcal{I}(\hat{s})} I(V_s; Y_s^n | U_s) - \max_{s \in \mathcal{I}(\hat{s})} I(V_s; Z_s^n | U_s) \right],$$

which completes the proof. ■

*Proof of Theorem 3:* The achievability of the SK rate in (11) for a finite source follows directly from the special case of Theorem 1. By taking RV  $U_{\hat{s}}$  to be  $X_{\hat{s}}$  in part a) of the proof of Theorem 1 in (54), it follows that the given rate in (11) for a finite  $\mathcal{S}$  is achievable.

To show the achievability of the SK rate in (11) for an infinite set of source states  $\mathcal{S}$  and a finite set of marginal states  $\hat{\mathcal{S}}$ , let  $\hat{s} \in \hat{\mathcal{S}}$  be given and consider the infinite class of stochastic matrices as follows:

$$\{P_{YZ,s|X_{\hat{s}}} : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{Y} \times \mathcal{Z})\}_{s \in \mathcal{I}(\hat{s})}. \quad (79)$$

Similarly as in [17], Lemma 5 implies that for any  $l > 2|\mathcal{Y} \times \mathcal{Z}|^2$ , there exists a finite set of stochastic matrices  $\{W_{s'} : \mathcal{X} \rightarrow \mathcal{P}(\mathcal{Y} \times \mathcal{Z})\}_{s' \in \mathcal{I}'(\hat{s})}$ , with  $|\mathcal{I}'(\hat{s})| \leq (l+1)^{|\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}|}$ , which approximates the one in (79) such that

$$\begin{aligned} \forall s \in \mathcal{I}(\hat{s}), \exists s' \in \mathcal{I}'(\hat{s}), \forall (x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}, \\ |P_{YZ,s|X_{\hat{s}}}(y, z|x) - W_{s'}(y, z|x)| \leq \frac{1}{l} |\mathcal{Y} \times \mathcal{Z}|, \end{aligned} \quad (80)$$

$$P_{YZ,s|X_{\hat{s}}}(y, z|x) \leq e^{\frac{2|\mathcal{Y} \times \mathcal{Z}|^2}{l}} W_{s'}(y, z|x). \quad (81)$$

As  $\hat{s} \in \hat{\mathcal{S}}$  was chosen arbitrarily, we may repeat this procedure for all  $\hat{s} \in \hat{\mathcal{S}}$  and define the following finite source

$$\mathfrak{G}' := \{XYZ, s'\}_{s' \in \mathcal{I}'(\hat{s}), \hat{s} \in \hat{\mathcal{S}}},$$

where for all  $\hat{s} \in \hat{\mathcal{S}}, s' \in \mathcal{I}'(\hat{s})$ , and  $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}$ , the PD of  $\mathfrak{G}'$  is given by

$$P_{XYZ,s'}(x, y, z) := P_{X_{\hat{s}}}(x) W_{s'}(y, z|x).$$

Define for a marginal index  $\hat{s}$  and indices  $r, t \in \mathcal{I}(\hat{s})$ ,

$$f(\hat{s}, r, t) := I(X_{\hat{s}}; Y_r) - I(X_{\hat{s}}; Z_t). \quad (82)$$

Since  $\mathfrak{G}'$  is a finite source, the following SK rate is again by using Theorem 1 achievable:

$$\min_{\hat{s} \in \hat{\mathcal{S}}} \min_{r', t' \in \mathcal{I}'(\hat{s})} f(\hat{s}, r', t').$$

In the following, it is shown that the SK generation protocol which guarantees the achievability of this SK rate for the finite source  $\mathfrak{G}'$ , also guarantees the achievability of the SK rate given in (11) for the infinite source  $\mathfrak{G}$  when  $l = n^3$ .

By using (80) and taking  $l = n^3$ , it follows for all  $r, t \in \mathcal{I}(\hat{s})$  and their corresponding indices  $r', t' \in \mathcal{I}'(\hat{s})$  that

$$\begin{aligned} \gamma_1 &:= \frac{1}{2} \|P_{XY,r} - P_{XY,r'}\| \leq \frac{1}{2n^3} |\mathcal{Y} \times \mathcal{Z}|^2, \\ \gamma_2 &:= \frac{1}{2} \|P_{XZ,t} - P_{XZ,t'}\| \leq \frac{1}{2n^3} |\mathcal{Y} \times \mathcal{Z}|^2. \end{aligned}$$

Since  $\gamma_1 \leq 1 - (|\mathcal{X}||\mathcal{Y}|)^{-1}$  and  $\gamma_2 \leq 1 - (|\mathcal{X}||\mathcal{Z}|)^{-1}$  hold for  $n$  large enough, it follows by Lemma 6 that

$$|I(X_{\hat{s}}; Y_r) - I(X_{\hat{s}}; Y_{r'})| \leq 3\gamma_1 \log(|\mathcal{X} \times \mathcal{Y}|) + 3h(\gamma_1), \quad (83)$$

$$|I(X_{\hat{s}}; Z_t) - I(X_{\hat{s}}; Z_{t'})| \leq 3\gamma_2 \log(|\mathcal{X} \times \mathcal{Z}|) + 3h(\gamma_2). \quad (84)$$

By using (82), (83), and (84), it holds that

$$\begin{aligned} &|f(\hat{s}, r, t) - f(\hat{s}, r', t')| \\ &\leq |I(X_{\hat{s}}; Y_r) - I(X_{\hat{s}}; Y_{r'})| + |I(X_{\hat{s}}; Z_t) - I(X_{\hat{s}}; Z_{t'})| \\ &\leq \frac{3|\mathcal{Y} \times \mathcal{Z}|^2}{2n^3} \log(|\mathcal{X}^2 \times \mathcal{Y} \times \mathcal{Z}|) + 6h\left(\frac{|\mathcal{Y} \times \mathcal{Z}|^2}{2n^3}\right). \end{aligned} \quad (85)$$

As stated before, the protocol related to the finite source  $\mathfrak{G}'$ , is used for the infinite source  $\mathfrak{G}$ . To show that the SK rate of this protocol is close to the one which is given in (11), it is sufficient to show that for a given  $\epsilon > 0$  it holds:

$$\left| \min_{\hat{s} \in \hat{\mathcal{S}}} \inf_{r, t \in \mathcal{I}(\hat{s})} f(\hat{s}, r, t) - \min_{\hat{s} \in \hat{\mathcal{S}}} \min_{r', t' \in \mathcal{I}'(\hat{s})} f(\hat{s}, r', t') \right| < \epsilon. \quad (86)$$

Let  $\tau > 0$  be given. There exist then  $r_0, t_0 \in \mathcal{I}(\hat{s})$  such that

$$\begin{aligned} \inf_{r, t \in \mathcal{I}(\hat{s})} f(\hat{s}, r, t) &> f(\hat{s}, r_0, t_0) - \tau \\ &\geq \min_{r', t' \in \mathcal{I}'(\hat{s})} f(\hat{s}, r', t') - \epsilon, \end{aligned}$$

where the second inequality holds for  $\tau$  small enough and is a result of (85) and the concavity of entropy. Similarly, there exist  $r'_0, t'_0 \in \mathcal{I}'(\hat{s})$  such that

$$\begin{aligned} \min_{r', t' \in \mathcal{I}'(\hat{s})} f(\hat{s}, r', t') &\geq f(\hat{s}, r'_0, t'_0) - \tau \\ &> \inf_{r, t \in \mathcal{I}(\hat{s})} f(\hat{s}, r, t) - \epsilon. \end{aligned}$$

Therefore, as the index  $\hat{s} \in \hat{\mathcal{S}}$  was taken arbitrarily, the relation (86) follows directly. This implies that condition (2) of Definition 4 is satisfied for the infinite source  $\mathfrak{G}$ .

For verifying condition (3) of Definition 4, the following inequality is required which follows by using (81):

$$\begin{aligned} P_{Y_{\hat{s}}|X_{\hat{s}}}^n(y^n|x^n) &= \prod_{i=1}^n P_{Y_{\hat{s}}|X_{\hat{s}}}(y_i|x_i) \\ &\leq e^{\frac{2|\mathcal{Y} \times \mathcal{Z}|^2 n}{l}} V_{s'}^n(y^n|x^n), \end{aligned} \quad (87)$$

where  $V_{s'}(y|x) := \sum_{z \in \mathcal{Z}} W_{s'}(y, z|x)$  for any  $x \in \mathcal{X}, y \in \mathcal{Y}$ .

In order to use the finite protocol for the infinite source  $\mathfrak{G}$ , the PD of the marginal RV  $X$  is estimated by Alice. Let the correct estimation decision be given by  $\hat{s}$ . The result of estimation for the source  $\mathfrak{G}$  is identical with the one from the source  $\mathfrak{G}'$ . Moreover, assume that the encoder  $g$  and decoder  $\tilde{g}$  which are given by Lemma 7a), are used to generate the CR. The error probability upper-bound for all  $s \in \mathcal{I}(\hat{s})$  is given by

$$\begin{aligned} &\Pr\{g(X_{\hat{s}}^n) \neq \tilde{g}(f(X_{\hat{s}}^n), \hat{S}_{\hat{s}}, Y_s^n)\} \\ &\leq P_{XY,s}^n(\{(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : g(x^n) \neq \tilde{g}(f(x^n), \hat{s}, y^n)\}) \\ &\quad + \sum_{\hat{s} \in \hat{\mathcal{S}} - \{\hat{s}\}} P_{\hat{S}_{\hat{s}}}(\hat{s}) \Pr\{g(X_{\hat{s}}^n) \neq \tilde{g}(f(X_{\hat{s}}^n), \hat{S}_{\hat{s}}, Y_s^n) | \hat{S}_{\hat{s}} = \hat{s}\} \\ &\leq e^{\frac{2|\mathcal{Y} \times \mathcal{Z}|^2}{l} n} \times P_{X_{\hat{s}}}^n(x^n) \times V_{s'}^n(\{(y^n \in \mathcal{Y}^n : \\ &\quad g(x^n) \neq \tilde{g}(f(x^n), \hat{s}, y^n)\} | x^n) + \exp(-nc_1) \cdot |\hat{\mathcal{S}}| \\ &\leq e^{\frac{2|\mathcal{Y} \times \mathcal{Z}|^2}{l} n} \times P_{XY,s'}^n(\{(x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : \\ &\quad g(x^n) \neq \tilde{g}(f(x^n), \hat{s}, y^n)\}) + \exp(-nc_1) \cdot |\hat{\mathcal{S}}| \\ &\leq e^{\frac{2|\mathcal{Y} \times \mathcal{Z}|^2}{n^2}} \exp(-n\delta_0) + \exp(-nc_1) \cdot |\hat{\mathcal{S}}|, \end{aligned}$$

for some  $c_1, \delta_0 > 0$ . The second inequality follows by (87) and (58). The last inequality is a result of (17) from Lemma 7a) and that  $l = n^3$ . Therefore, the error probability is exponentially small. Furthermore, as  $|\mathcal{I}'(\hat{s})| < (l+1)^{|\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}|}$  and  $l = n^3$ , a universal  $\delta_1$  exists for which the probability in (32) is non-zero and thus such a coding scheme for the finite source  $\mathfrak{G}'$  exists.

To show that condition (4) of Definition 4 is also guaranteed, assume again that the encoder  $g$  and decoder  $\tilde{g}$  from Lemma 7a) are used and the correct estimation decision is  $\hat{s}$ . As the protocol guarantees condition (4) of Definition 4 for the finite source  $\mathfrak{S}'$ , it holds by using Definitions 3 for all  $\epsilon_0 > 0$ ,  $n$  sufficiently large, and  $s' \in \mathcal{I}'(\hat{s})$  that

$$S(K_A|Z_{s'}^n, f(X_{\hat{s}}^n), \hat{S}_{\hat{s}} = \hat{s}) = \log |\mathcal{K}| - H(\kappa(g(X_{\hat{s}}^n))|\hat{S}_{\hat{s}} = \hat{s}) + I(\kappa(g(X_{\hat{s}}^n)); Z_{s'}^n, f(X_{\hat{s}}^n)|\hat{S}_{\hat{s}} = \hat{s}) < \epsilon_0, \quad (88)$$

where  $K_A, \mathcal{K}$ , and  $\kappa$  are given by Definition 2 and Lemma 8. Furthermore, it holds that

$$\begin{aligned} \gamma_3 &:= \frac{1}{2} \left\| \mathbb{P}_{\kappa(g(X_{\hat{s}}^n))Z_{\hat{s}}^n f(X_{\hat{s}}^n)|\hat{S}_{\hat{s}}(\cdot|\hat{s})} - \mathbb{P}_{\kappa(g(X_{\hat{s}}^n))Z_{s'}^n f(X_{\hat{s}}^n)|\hat{S}_{\hat{s}}(\cdot|\hat{s})} \right\| \\ &\leq \frac{1}{2 - 2\exp(-nc_0)} \left\| \mathbb{P}_{\kappa(g(X_{\hat{s}}^n))Z_{\hat{s}}^n f_c(X_{\hat{s}}^n)} - \mathbb{P}_{\kappa(g(X_{\hat{s}}^n))Z_{s'}^n f_c(X_{\hat{s}}^n)} \right\| \\ &\leq \frac{n \left\| \mathbb{P}_{XZ, s} - \mathbb{P}_{XZ, s'} \right\|}{2 - 2\exp(-nc_0)} \leq \frac{|\mathcal{Y} \times \mathcal{Z}|^2}{2n^2(1 - \exp(-nc_0))}, \end{aligned} \quad (89)$$

where RVs  $f(X_{\hat{s}})$  with alphabet  $\mathcal{I}$  and  $f_c(X_{\hat{s}}^n) = (f(X_{\hat{s}}^n), \hat{S}_{\hat{s}})$  are given by Lemma 7a) and proof of Theorem 1. The first inequality follows by (57) and the second one by the fact that no mapping of the PDs increases their 1-norm distance. The last inequality is a result of (80) and that  $l = n^3$ . Since  $\gamma_3 \leq 1 - \frac{1}{|\mathcal{K} \times \mathcal{Z}^n \times \mathcal{I}|}$ , then for all  $\epsilon_1 > 0$ , Lemma 6 implies by using (89) that

$$\begin{aligned} &|I(\kappa(g(X_{\hat{s}}^n)); Z_{s'}^n, f(X_{\hat{s}}^n)|\hat{S}_{\hat{s}} = \hat{s}) \\ &\quad - I(\kappa(g(X_{\hat{s}}^n)); Z_{\hat{s}}^n, f(X_{\hat{s}}^n)|\hat{S}_{\hat{s}} = \hat{s})| \\ &\leq 3\gamma_3 \log(|\mathcal{K} \times \mathcal{Z}^n \times \mathcal{I}| - 1) + 3h(\gamma_3) \\ &\leq \frac{3|\mathcal{Y} \times \mathcal{Z}|^2 c_2}{2n(1 - \exp(-nc_0))} + 3h\left(\frac{|\mathcal{Y} \times \mathcal{Z}|^2}{2n^2(1 - \exp(-nc_0))}\right) < \epsilon_1, \end{aligned} \quad (90)$$

for some  $c_2 > 0$  and  $n$  sufficiently large. The second inequality follows by the fact that the argument of the log function does not increase faster than exponentially. Therefore, it follows by using (88) and (90) that for all  $s \in \mathcal{I}(\hat{s})$ ,

$$S(K_A|Z_s^n, f(X_{\hat{s}}^n), \hat{S}_{\hat{s}} = \hat{s}) < \epsilon_0 + \epsilon_1.$$

This inequality together with (58) implies for all estimation results which may lead to a correct or incorrect decision that

$$\begin{aligned} S(K_A|Z_s^n, f(X_{\hat{s}}^n), \hat{S}_{\hat{s}}) &= \mathbb{P}_{\hat{S}_{\hat{s}}}(\hat{s}) S(K_A|Z_s^n, f(X_{\hat{s}}^n), \hat{S}_{\hat{s}} = \hat{s}) \\ &\quad + \sum_{\tilde{s} \in \hat{\mathcal{S}} - \{\hat{s}\}} \mathbb{P}_{\hat{S}_{\hat{s}}}(\tilde{s}) S(K_A|Z_s^n, f(X_{\hat{s}}^n), \hat{S}_{\hat{s}} = \tilde{s}) \\ &\leq \epsilon_0 + \epsilon_1 + |\hat{\mathcal{S}}| \exp(-nc_1). \end{aligned}$$

The existence of the SK generator  $\kappa$  for the finite source  $\mathfrak{S}'$  follows by applying the relation  $|\mathcal{I}'(\hat{s})| < (n^3 + 1)^{|\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}|}$  to (39) and (69), so that the probability in (53) is non-zero.

For the converse proof, assume that  $R_{\text{sk}}$  is achievable. The result from [4, Theorem 1] implies that

$$R_{\text{sk}} \leq \min_{\hat{s} \in \hat{\mathcal{S}}} \inf_{r, t \in \mathcal{I}(\hat{s})} I(X_{\hat{s}}; Y_r | Z_t). \quad (91)$$

Furthermore, for any given  $\hat{s} \in \hat{\mathcal{S}}$  and all  $r, t \in \mathcal{I}(\hat{s})$ , it holds by (10) that

$$I(X_{\hat{s}}; Y_r) - I(X_{\hat{s}}; Z_t) = I(X_{\hat{s}}; Y_r | Z_t).$$

This identity together with (91) completes the proof. ■

## V. CONCLUSION

The SK generation protocol which was introduced in this work used a two phase approach to achieve the given SK rate. In the first step, Alice estimated her state and sent this along with other information which was obtained from her observation to Bob. Although, this information is also received by Eve, it was shown that the strong secrecy and uniformity of the generated SK is still guaranteed. In the second step, Bob used this information including the estimated state of Alice to generate the SK. A single-letter lower-bound for the SK capacity of a finite compound source was derived as a function of the communication rate constraint between Alice and Bob. This result was further extended to a multi-letter SK capacity formula by discarding the public communication rate constraint. As the final result, a single-letter SK capacity formula was derived for degraded compound sources with no communication constraint and an arbitrary set of source states. It was shown that for any infinite compound source, with finite marginal set of states, there exists an approximating finite source whose SK generation protocol also guarantees the achievability of the given rates for the infinite source.

## REFERENCES

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, 1949.
- [2] P. Gács and J. Körner, "Common information is far less than mutual information," *Problems of Control and Information Theory*, vol. 2, pp. 149–162, 1973.
- [3] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [4] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - part I: Secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.
- [5] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 344–366, March 2000.
- [6] —, "Secrecy capacities for multiple terminals," *IEEE Transactions on Information Theory*, vol. 50, no. 12, pp. 3047–3061, December 2004.
- [7] I. Csiszár and J. Körner, *Information Theory, Coding Theorems for Discrete Memoryless Systems*, 2nd ed. Cambridge Uni. Press, 2011.
- [8] T. Ignatenko and F. M. Willems, "Biometric security from an information-theoretical perspective," *Foundations and Trends in Communication and Information Theory*, vol. 7, no. 2, pp. 135–316, 2012.
- [9] L. Lai, S.-W. Ho, and H. V. Poor, "Privacy-security trade-offs in biometric security systems-part I: Single use case," *IEEE T-IFS*, vol. 6, no. 1, pp. 122–139, December 2010.
- [10] R. Wilson, D. Tse, and R. A. Scholtz, "Channel identification: Secret sharing using reciprocity in ultrawideband channels," *IEEE Transactions on Information Forensics and Security*, vol. 2, no. 3, pp. 364–375, September 2007.
- [11] M. Bloch, "Channel intrinsic randomness," in *Proc. IEEE International Symposium on Information Theory*, June 2010, pp. 2607–2611.
- [12] H. Boche and R. F. Wyrembelski, "Secret key generation using compound sources - optimal key-rates and communication costs," in *Proc. 9th International ITG Conference on Systems, Communication and Coding (SCC)*, January 2013, pp. 1–6.
- [13] J.-H. Jahn, "Kodierung beliebig variierender korrelierter Quellen," Ph.D. dissertation, Universität Bielefeld, Fakultät für Mathematik, 1978.
- [14] S. C. Draper and E. Martinian, "Compound conditional source coding, slepian-wolf list decoding, and applications to media coding," in *Proc. IEEE International Symposium on Information Theory*, June 2007, pp. 1511–1515.
- [15] R. A. Chou and M. R. Bloch, "Secret-key generation with arbitrarily varying eavesdroppers channel," in *Proc. IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, December 2013, pp. 277–280.

- [16] I. Bjelaković, H. Boche, and J. Sommerfeld, "Secrecy results for compound wiretap channels," *Problems of Information Transmission*, vol. 49, no. 1, pp. 73–98, 2013.
- [17] R. F. Schaefer and S. Loyka, "The secrecy capacity of compound gaussian MIMO wiretap channels," *IEEE Transactions on Information Theory*, vol. 61, no. 10, pp. 5535–5552, July 2015.
- [18] A. Grigorescu, "Robust biometric authentication and secure message transmission," Master's thesis, Technische Universität München, Lehrstuhl für Theoretische Informationstechnik, February 2015.
- [19] N. Tavangaran, H. Boche, and R. F. Schaefer, "Secret-key capacity of compound source models with one-way public communication," in *Proc. IEEE ITW, Jeju Island, Korea*, October 2015.
- [20] U. M. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," *EUROCRYPT 2000, Lecture Notes in Computer Science*, Springer-Verlag, vol. 1807, pp. 351–368, May 2000.
- [21] W. Hoeffding, "Asymptotically optimal tests for multinomial distributions," *Annals of Mathematical Statistics*, vol. 36, pp. 369–401, 1965.
- [22] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography - part II: CR capacity," *IEEE Transactions on Information Theory*, vol. 44, no. 1, pp. 225–240, January 1998.
- [23] D. Blackwell, L. Breiman, and A. J. Thomasian, "The capacity of a class of channels," *The Annals of Mathematical Statistics*, vol. 30, no. 4, pp. 1229–1241, December 1959.
- [24] Z. Zhang, "Estimating mutual information via kolmogorov distance," *IEEE Transactions on Information Theory*, vol. 53, no. 9, pp. 3280–3282, September 2007.
- [25] I. Csiszár, "Almost independence and secrecy capacity," *Problems of Information Transmission*, vol. 32, no. 1, pp. 48–57, 1996.
- [26] A. N. Shiryaev, *Probability*, 2nd ed. Springer, 1995.
- [27] M. Fekete, "Über die verteilung der wurzeln bei gewissen algebraischen gleichungen mit ganzzahligen koeffizienten," *Mathematische Zeitschrift*, vol. 17, pp. 228–249, 1923.